Seminar Stiinta informatica

UNIVERSITATEA "AL.I.CUZA" IASI

FACULTATEA DE MATEMATICA - MECANICA

SEMINARUL DE TEORIA AUTOMATELOR SI LIMBAJELOR FORMALE

- 2 -

CORINA REISCHER DAN SIMOVICI

E L E M E N T E

D E

T E O R I A G E N E R A L A A C O D U R I L O R

- 1973 -

C U P R I N S

Introducere 7

I.Preliminarii

§ I.1. Noţiunea de cod 12
§ I.2. Aplicaţii asociate unui cod 16
§ I.3. Clase speciale de coduri. 26

II.Coduri cu lungime variabilă pentru canale fără zgomot.

§ II.1. Coduri cu unică descifrabilitate 37
§ II.2. Teoremele lui Sardinas - Patterson şi Levenştein de unică descifrabilitate 44
§ II.3. Unica descifrabilitate infinită şi ciclică 59
§ II.4. Coduri decodabile. 67
§ II.5. Coduri sincronizabile. 73

III.Coduri cu lungime variabilă pentru canale cu zgomot.

§ III.1. Noţiunea de mulţime calibrată 80
§ III.2. Siruri de mulţimi calibrate 93
§ III.3. Coduri corectoare. 104
§ III.4. Coduri decodabile. 107
§ III.5. Coduri sincronizabile. 110

Anexa A. Semigrupuri libere 116
Bibliografie 125
Indice alfabetic 133

CONTENT

Introduction 7

I. Preliminaries . . . . . .

§ I. 1. The notion of code. 12

§ I. 2. Mappings associated to a code 16

§ I. 3. Special classes of codes. 26

II. Variable length codes for noiseless channels . . . . . .

§ II. 1. Codes with unique decipherability 37

§ II. 2. The theorems of Sardinas - Patterson and Levenshtein of unique decipherability . . . 44

§ II. 3. Infinite and cyclic unique decipherability. . . 59

§ II. 4. Decodable codes 67

§ II. 5. Synchronizable codes. 73

III. Variable length codes for noisy channels. .

§ III. 1. The notion of gauged set 80

§ III. 2. Sequences of gauged sets. 93

§ III. 3. Correcting codes. 104

§ III. 4. Decodable codes 107

§ III. 5. Synchronizable codes. 110

Appendix A. Free semigroups 116

References 125

Alphabetic index. 133

INTRODUCERE

Teoria codurilor este o disciplină matematică care face parte din ansamblul de discipline cunoscute astăzi sub numele de Informatică. Ea se ocupă cu studiul algebric al fenomenului de transmitere a informaţiei.

Schema generală a unui sistem de transmitere a informaţiei se compune din cinci elemente: sursa de informaţie, dispozitivul de codificare, canalul de transmitere, dispozitivul de decodificare şi receptorul (v.fig.1).

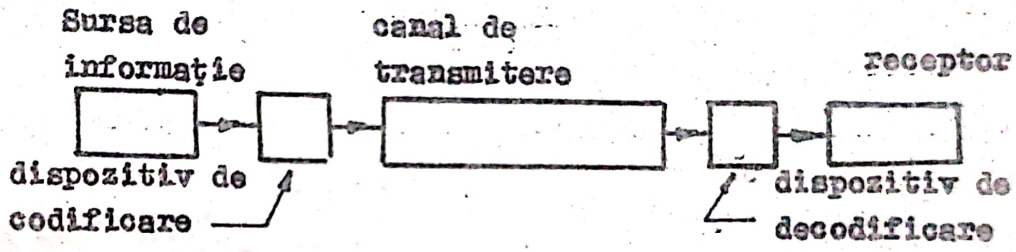


Fig.1

Sursa de informaţie produce un mesaj. Mesajul este dat în general sub formă de şiruri finite, în scrierea binară (prin folosirea cifrelor 0 şi 1), zecimală (prin folosirea cifrelor $0, 1, \ldots, 9$) sau într-un alfabet oarecare I, în acest ultim caz mesajul fiind format din cuvinte din I^*, semigrupul liber generat de I.

Rolul dispozitivului de codificare este acela de a transforma semnalele mesajului emis de sursă în semnale susceptibile de a se propaga prin canalul de transmitere a informaţiei.

Canalul este un sistem care permite să se vehiculeze de la intrarea la ieşirea sa, un număr finit de semnale, care pot fi diferite manifestări ale unui fenomen fizic (semnale elec-

trice de o anumită formă cu anumite restricţii asupra caracteristicelor - de exemplu,asupra puterii, duratei, lărgimei benzii -, variaţiile unui cîmp magnetic, semnele optice, acustice etc.).

Dispozitivul de decodificare transformă semnalele primite prin canalul de transmitere în semnale acceptate de receptor.

In timpul transmiterii prin canal a unui cuvînt din I'', pot apare perturbaţii, aşa fel încît cuvîntul introdus în canal să difere de cuvîntul primit, apărînd astfel erori de transmitere.

Canalele în care pot apărea asemenea fenomene se numesc canale cu zgomot; canalele pentru care cuvîntul intrat în canal coincide totdeauna cu cel ieşit se numesc canale fără zgomot.

Canalele reale sînt în general canale cu zgomot.

Pentru a se contracara influenţa zgomotelor în canale şi pentru a se putea reconstitui la ieşire cuvintele introduse în canal este necesar ca alegerea cuvintelor din I'', care se folosesc în transmitere să fie făcută după anumite considerente, dintre care unele vor fi prezentate în această lucrare.

Mulţimile de cuvinte folosite la transmitere pot consta fie din cuvinte de lungimi diferite (coduri cu lungime variabilă) fie din cuvinte de aceeaşi lungime (coduri bloc). Disciplina care se ocupă cu studiul acestor mulţimi se numeşte teoria codurilor.

Printre tipurile de erori care pot apare în timpul transmiterii, distingem:

-erori de substituţie, în cazul în care unii simboli din cuvîntul transmis, sînt înlocuiţi prin alţi simboli, menţinîndu-se constantă lungimea cuvîntului.

-erori de sincronizare, în cazul în care unele subcuvinte ale cuvîntului transmis sînt înlocuite prin altele,de lungime diferită, cuvîntul la ieşire fiind de lungime diferită de lungimea cuvîntului de la intrare.

-erori de stergere, în cazul în care unii simboli din cuvîntul transmis sînt înlocuiţi cu simboli care nu aparţin alfabetului folosit la transmitere (presupus a fi inclus strict în alfabetul I).

Se presupune în general, că fiecare simbol din cuvîntul transmis este afectat independent de zgomot, şi deci probabilitatea unei erori de un anumit tip, depinde numai de numărul simbolilor afectaţi, deci de numărul erorilor elementare (erori care afectează un singur simbol).

Alegerea cuvintelor care urmează a fi transmise se face tocmai în vederea corectării şi detectării erorilor.

Teoria codurilpr s-a dezvoltat în două direcţii diferite.

1)Imbunătăţirea comunicaţiilor în canale cu zgomot, ceea ce a revenit la studiul codurilor corectare de erori, care sînt totdeauna presupuse coduri bloc.

2)Cercetarea unor aspecte de bază ale comunicaţiilor ca: unica descifrabilitate, sincronizare etc. ceea ce a revenit la studiul codurilor cu lungime variabilă, dar canalele sînt presupuse fără zgomot.

Incepînd din anul 1964 un grup de matematicieni de la Parke Mathematical Laboratories, Carlisle, Massachusetts a întreprins un studiu al codurilor cu lungime variabilă pentru canale cu zgomot, dezvoltînd o teorie generală a transmiterii informaţiei în canalele cu zgomot care generalizează rezultatele clasice din studiul codurilor cu lungime variabilă pentru canale fără zgomot.

In această lucrare vom sintetiza rezultatele obţinute în teoria codurilor cu lungime variabilă pentru canale fără zgomot şi canale cu zgomot.

Scanned with OKEN Scanner

Menţionăm că teoria codurilor cu lungime variabilă este cunoscută în literatura de specialitate şi sub numele de teoria generală a codurilor.

Recomandăm parcurgerea prealabilă a anexei care conţine unele rezultate de teoria semigrupurilor libere, folosite efectiv în lucrare.

Bibliografia indică la sfîrşitul lucrării este aproape exhaustivă. Mulţumim cu acest prilej D-lui Prof. W.E. Hartnett care ne-a oferit cu amabilitate unele lucrări ale grupului de matematicieni de la Parke Mathematical Laboratories, Carlisle, Massachusetts.

Scanned with OKEN Scanner

Partea I-a

Preliminarii

Scanned with OKEN Scanner

§ I. 1. Noţiunea de cod

Fie I un alfabet cu $|I| \geq 2$, I^* semigrupul liber generat de I, $H \subseteq I^* \setminus \{e\}$ şi H^* semigrupul liber generat de H.

Definiţia I.1.1. O aplicaţie de admisibilitate pe H^*, este o aplicaţie $\alpha : H^* \longrightarrow P(I^*)$, astfel încît $\forall r \in I^*$, $p, q \in H$ şi $m, n \in H^*$, să avem îndeplinite condiţiile:

i) $\hat{m} \in \alpha(m)$,

ii) dacă $r \in \alpha(m) \Rightarrow \ell(r) = \ell(\hat{m})$,

iii) dacă $\alpha(p) \cap \alpha(q) \neq \emptyset \Rightarrow p = q$,

iv) $\alpha(mn) = \alpha(m)\,\alpha(n)$.

Observaţia I.1.1. Condiţia iv) asigură că o aplicaţie de admisibilitate este un homomorfism între semigrupurile H^* şi $P(I^*)$. Prin urmare aplicaţia α este unic determinată prin valorile pe care le ia pe mulţimea de generatori H.

Observaţia I.1.2. Aplicaţia $\iota : H^* \longrightarrow P(I^*)$, dată prin $\iota(m) = \{\hat{m}\}$, este o aplicaţie de admisibilitate pe H^*.

Definiţia I.1.2. Un cod pe alfabetul I este o pereche (H, α) unde $H \subseteq I^* \setminus \{e\}$, iar α este o aplicaţie de admisibilitate pe H.

Dacă $\alpha = \iota$, atunci perechea (H, ι) se numeşte cod simplu.

Convenim să notăm (H, ι) prin H şi $\iota(m) = \{\hat{m}\}$ prin $\hat{m}$.

Dacă $|I| = 2$, se obţin codurile binare.

După cum mulţimea H este finită sau infinită, se obţin coduri finite sau coduri infinite.

Ne vom ocupa în special de coduri finite pe care le vom numi pe scurt, coduri.

Definiţia I.1.3. Dacă (H, α) este un cod, atunci orice

cuvînt $p \in H$ se numeşte cuvînt-cod , iar orice propoziţie $m \in H^*$, mesaj .Mulţimea $\propto(m)$ este $\propto$ -domeniul (pe scurt,domeniul) de admisibilitate al lui m, iar orice element $v \in \propto(m)$ este $\propto$ -admisibil (pe scurt admisibil).

Observaţia I.1.3. Dacă $(H, \propto)$ este un cod, atunci domeniul de admisibilitate al unui cuvînt $p \in H$, deci $\propto(p)$, se interpretează ca fiind format din acele cuvinte din I^*, care atunci cînd sînt recepţionate se decodifică în p; altfel exprimat $\propto(p)$ este format din acele cuvinte din I^*, care sînt posibile de a fi recepţionate,atunci cînd este transmis cuvîntul p. Dacă $v \in \propto(p)$, diferenţa dintre p şi v este un model de eroare, descris de aplicaţia $\propto$.

In mod analog se interpretează $\propto(m)$,cu $m \in H^*$.

Observaţia I.1.4.Pentru codurile simple H, avem $\propto(p) = \{p\}$, $\forall p \in H$, prin urmare cînd este transmis cuvîntul cod p, se recepţionează tot cuvîntul p, cuvîntul - cod nefiind afectat de erori, canalul de transmitere fiind în acest caz fără zgomot.

Observaţia I.1.5. Condiţia i)din definiţia I.1.1,presupune că atunci cînd se transmite un cuvînt-cod (sau un mesaj) şi este recepţionat corect să fie decodificat în cuvîntul (sau mesajul) transmis, cerinţă naturală în transmiterea de informaţie.

Observaţia I.1.6.Condiţia ii) din definiţia I.1.1 cere ca toate cuvintele admisibile pentru un cuvînt-cod,$p \in H$, să aibă aceiaşi lungime cu p, deci pot fi corectate în acest fel numai erorile de substituţie.

Observaţia I.1.7. Condiţia iii) din definiţia I.1.1, în cazul codurilor simple, revine la faptul că toate cuvintele

-cod sînt distincte, iar pentru coduri $(H, \propto)$ asigură că de-codificarea unui cuvînt recepţionat se face fără ambiguitate deoarece un cuvînt nu poate aparţine la două domenii de admisibilitate corespunzătoare la două cuvinte-cod.

Atragem atenţia asupra faptului că această condiţie nu asigură că atunci cînd se transmite un mesaj, decodificarea se face fără ambiguitate. Următorul exemplu justifică afirmaţia făcută.

Exemplul I.1.1. Fie $I = \{0, 1, 2\}$ şi $H = \{0, 02\}$.

Deoarece $\ell(0) = 1$ şi $\ell(02) = 2$, şi orice aplicaţie de admisibilitate $\propto$ păstrează lungimea cuvintelor, avem $\propto(0) \cap \propto(02) = \emptyset$, deci este îndeplinită condiţia iii).

Fie $\propto(0) = \{0,1\}$ şi $\propto(02) = \{02, 12, 01, 11\}$, deci aplicaţia de admisibilitate aleasă, poate corecta erorile în care $0 \to 1$, $1 \to 0$ sau $1 \to 2$ şi $2 \to 1$.

Dacă se recepţionează 01, atunci nu se poate decide dacă a fost transmis mesajul 00 sau cuvîntul 02, deci există ambiguitate în decodificarea mesajelor.

Pentru a se elimina această situaţie, în transmitere se folosesc coduri speciale (v.§ I.3).

Definiţia I.1.4. Codul extins al codului $(H, \propto)$ este codul simplu $(\propto(H), \iota)$, unde $\propto(H) = \bigcup\{\propto(p) \mid p \in H\}$ şi ι este aplicaţia din observaţia I.2.2.

Definiţia I.1.5. Mulţimea de şiruri admisibile pentru codul $(H, \propto)$ este

$$\Omega(H, \propto) = \bigcup\{\propto(m) \mid m \in H^*\}.$$

Observaţia I.1.8. Avem $\Omega(H, \propto) = \propto(H^*) = \widehat{(\propto(H)^*)}$.

In adevăr $z \in \propto(H^*) \iff \exists\ m = (p_1, \ldots p_k) \in H^*$ şi $z \in \propto(m) \iff$

$z \in (p_1)\ldots \propto (p_k) \Leftrightarrow z = z_1 \ldots z_k$ cu $z_j \in \propto(p_j)$, $j = \overline{1,k} \Longleftrightarrow$ $z = \widehat{(z_1,\ldots,z_k)}$ şi $z_j \in \propto(p_j)$, $j = \overline{1,k} \Leftrightarrow z \in \widehat{(\propto(H))^*}$.

Mulţimea şirurilor admisibile $\Omega(H, \propto)$ este un subsemigrup al lui I^*, ca fiind imagine homomorfă a unui semigrup liber, şi anume a lui $(\propto(H))^*$, homomorfismul fiind aplicaţia $\wedge$.

Observaţia I.1.9. Codul extins al unui cod simplu (H, ι) coincide cu codul dat, iar mulţimea şirurilor admisibile este $\widehat{(H^*)}$.

Legătura dintre codul extins şi mulţimea şirurilor admisibile este dată în:

Teorema I.1.1. Avem $\Omega(H, \propto) = S(\propto(H))$.

Demonstraţie. Rezultă imediat din teorema A.2 şi din observaţia I.1.9. ■

Observaţia I.1.10. Avem $\Omega(\propto(H), \iota) = \iota((\propto(H))^*) = \widehat{(\propto(H))^*} = \Omega(H, \propto)$, deci mulţimile de şiruri admisibile pentru un cod şi codul său extins, coincid.

Deci pentru orice cod $(H, \propto)$ există un cod simplu cu aceeaşi mulţime de şiruri admisibile. Ca atare, pentru acele proprietăţi ale codurilor care decurg din mulţimea de şiruri admisibile, se poate folosi codul dat sau codul său extins. Mai mult, ţinînd intervine mulţimea de şiruri admisibile, putem presupune totdeauna că avem de a face cu un cod simplu.

Fie K mulţimea tuturor codurilor pe alfabetul I.

Definiţia I.1.6. Relaţia de extindere este $E \subseteq K \times K$ cu $((H_1, \propto'), (H_2, \propto")) \in E \Leftrightarrow (\propto'(H_1), \iota) = (\propto"(H_2), \iota)$, adică codurile $(H_1, \propto')$ şi $(H_2, \propto")$ au acelaşi cod extins.

Observaţia I.1.11. Relaţia de extindere este o relaţie de echivalenţă, adică reflexivă, simetrică şi tranzitivă. Vom nota

cu $[(H,\alpha)]$ clasa de echivalenţă a codului (H,α). Deoarece $(\alpha(H), \iota) \in [(H,\alpha)]$, în orice clasă de echivalenţă există cel puţin un cod simplu.

Definiţia I.1.7. O proprietate de cod este extensibilă dacă odată cu codul (H,α) orice cod din clasa de echivalenţă $[(H,\alpha)]$ posedă acea proprietate.

Observaţia I.1.12. Pentru orice proprietate extensibilă a unui cod (H,α) există un cod simplu care posedă acea proprietate. In adevăr, cel puţin codul extins $(\alpha(H), \iota)$ posedă proprietatea.

Proprietăţile extensibile au o importanţă deosebită în teoria codurilor, deoarece studiul lor se poate face pe un cod pentru un canal fără zgomot.

§ I.2.Aplicaţii asociate unui cod.

Fie (H,α) un cod şi $(\alpha(H), \iota)$ codul său extins.

Să considerăm aplicaţia $\gamma : \alpha(H) \to H$, dată prin $\gamma(v) = p \iff v \in \alpha(p)$. Condiţia iii) din definiţia I.1.1. asigură că γ este o aplicaţie, deoarece pentru orice $v \in \alpha(H)$ există un singur $p \in H$ cu $v \in \alpha(p)$. Mai mult γ este o aplicaţie surjectivă.

Definiţia I.2.1. Homomorfismul de corectare pentru codul (H, α) este homomorfismul surjectiv $\gamma^* : (\alpha(H))^* \to H^*$, extins în mod unic din aplicaţia $\gamma : \alpha(H) \to H$.

Dacă $v = (v_1, \ldots, v_k) \in (\alpha(H))^*$, atunci

$$\gamma(v) = (\gamma(v_1), \ldots, \gamma(v_k)) = (p_1, \ldots, p_k) \in H^* \iff$$

$$\iff v_j \in \alpha(p_j),\ j = \overline{1,k}.$$

Deoarece $H^* \subseteq (\alpha(H))^*$ putem considera $\gamma(m)$ pentru $m \in H^*$; avem, în acest caz, $\gamma(m) = m$, $\forall\, m \in H^*$.

In cazul codurilor simple (H, ι), un homomorfism de co-

rectare se reduce la aplicaţia identică $1_{H^*} : H^* \longrightarrow H^*$.

Observaţia I.2.1. Pentru price $v \in (\alpha(H))^*$ avem $\hat{v} \in \alpha\gamma(v)$. In adevăr dacă $v \in (\alpha(H))^*$, atunci $v = (v_1, \ldots, v_k)$ şi există $p_j \in H$, cu $v_j \in \alpha(p_j)$, $j = \overline{1,k}$. Atunci $\gamma(v) = (\gamma(v_1), \ldots, \gamma(v_k)) = (p_1, \ldots, p_k)$, iar $\alpha\gamma(v) = \alpha(p_1) \ldots \alpha(p_k)$. Pe de altă parte $\hat{v} = v_1 \ldots v_k \in \alpha(p_1) \ldots \alpha(p_k)$, deoarece $v_j \in \alpha(p_j)$, $j = \overline{1,k}$.

Mai mult v egalează pe $\gamma(v)$, deoarece v şi $\gamma(v)$ au acelaşi număr de cuvinte şi $l(v(j)) = l(\gamma(v)(j))$, $j = \overline{1,k}$.

Homomorfismul de corectare asociază fiecărui element $v \in (\alpha(H))^*$ deci fiecărei propoziţii pe $\alpha(H)$, un mesaj din H^*, adică o propoziţie pe H, care conţine în α - domeniul său pe $\hat{v}$.

Teorema I.2.1. Fiind dat $m \in H^*$ şi $z \in \alpha(m)$ există $v \in (\alpha(H))^*$, astfel încît $z = \hat{v}$ şi $\gamma(v) = m$.

Demonstraţie. Fie $m = (p_1, \ldots, p_r)$ şi $z \in \alpha(m)$. Atunci $z \in \alpha(p_1) \ldots \alpha(p_r)$, deci $z = z_1 \ldots z_r$, cu $z_j \in \alpha(p_j)$, $j = \overline{1,r}$. Prin urmare $z_j \in \alpha(H)$ şi $\gamma(z_j) = p_j$. Atunci $v = (z_1, \ldots, z_r) \in (\alpha(H))^*$. Prin construcţie avem $z = \hat{v}$ şi $\gamma(v) = (\gamma(z_1), \ldots, \gamma(z_r)) = (p_1, \ldots, p_r) = m$. ■

Definiţia I.2.2. O aplicaţie (homomorfism) de decodificare pentru codul (H, α) este o aplicaţie (homomorfism) $\delta : \Omega(H, \alpha) \longrightarrow H^*$ cu $z \in \alpha\delta(z)$, pentru orice $z \in \Omega(H, \alpha)$.

Aplicaţia de decodificare asociază unei propoziţii admisibile, un mesaj din H^*, în al cărui α - domeniu se găseşte propoziţia admisibilă dată.

Definiţia I.2.3. O aplicaţie (homomorfism) de scindare

pentru codul (H, α) este o aplicaţie (homomorfism) surjectivă $\sigma : \Omega(H, \alpha) \longrightarrow (\alpha(H))^*$, astfel că $z = \widehat{\sigma(z)}$, $\forall z \in \Omega(H;\alpha)$.

Avem deci $\wedge\sigma = 1_{\Omega(H,\alpha)}$, unde am notat prin $1_{\Omega(H,\alpha)}$ aplicaţia identică pe $\Omega(H, \alpha)$.

Aplicaţia de scindare are ca efect despărţirea (scindarea) unei propoziţii admisibile în cuvintele din $\alpha(H)$ din care este formată.

Observaţia I.2.2. O aplicaţie de scindare pentru codul (H, α) este o aplicaţie de decodificare pentru codul extins $(\alpha(H), \iota)$ deoarece $\iota(\sigma(z)) = \{\widehat{\sigma(z)}\}$ şi $z \in \iota(\sigma(z))$ dacă şi numai dacă $z = \widehat{\sigma(z)}$.

Pentru codurile simple noţiunile de aplicaţie de decodificare şi aplicaţie de scindare coincid. In adevăr fie (H, ι) un cod simplu, Atunci $\sigma : \Omega(H, \iota) \longrightarrow H^*$ este o aplicaţie de scindare pentru codul (H, ι) dacă şi numai dacă $\forall z \in \Omega(H, \iota)$ avem $z = \widehat{\sigma(z)}$, deci dacă şi numai dacă $z = \iota(\sigma(z))$, deci dacă şi numai dacă σ este o aplicaţie de decodificare pentru codul (H, ι).

In figura I.2.1. sînt reprezentate relaţiile dintre diversele aplicaţii introduse mai sus. Prin săgeţi neetichetate s-au notat aplicaţii de incluziune, prin săgeţi punctate corespondenţe multivalente, iar prin săgeţi cu două linii, cei doi paşi de decodificare (σ şi $\dagger$).

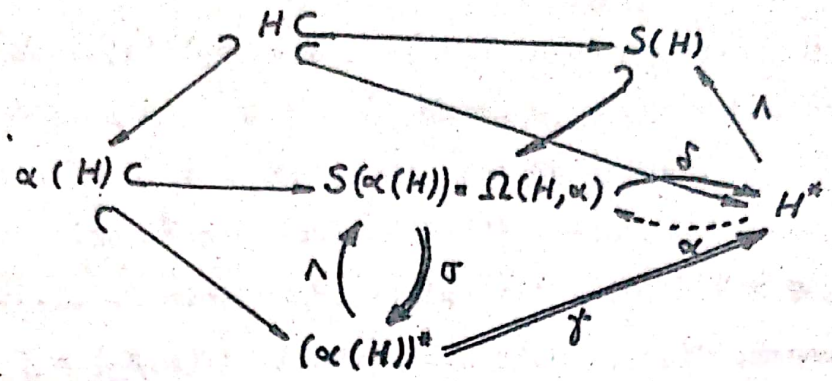
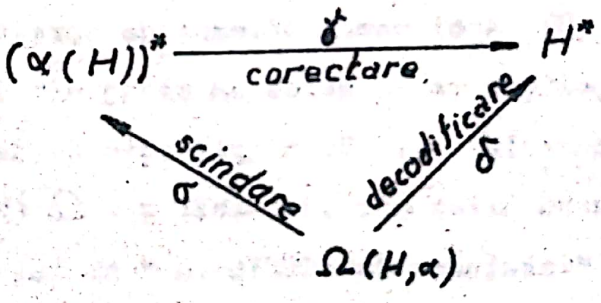


Fig. I.2.1.

Teorema I.2.2. Pentru fiecare aplicaţie de decodificare δ (scindare σ) pentru codul (H, α) există o aplicaţie de scindare σ (decodificare δ) pentru codul (H, α) astfel încît $\delta = \gamma\sigma$, deci pentru care triunghiul



este comutativ. Dacă aplicaţia σ este un homomorfism de scindare atunci aplicaţia δ este un homomorfism de decodificare.

Demonstraţie. Să presupunem că este dată aplicaţia de decodificare δ pentru codul (H, α). Vom defini aplicaţia σ, folosind teorema I.2.1. Astfel pentru $z \in \Omega(H, \alpha)$, $u \in \alpha\delta(z)$, punem $\sigma(z) = u$, dacă $\hat{u} = z$ şi $\gamma(u) = \delta(z)$. Deoarece $z = \widehat{\sigma(z)}$, σ este o aplicaţie de scindare pentru codul (H, α). Apoi $\delta(z) = \gamma(u) = \gamma\sigma(z)$, $\forall z \in \Omega(H, \alpha)$, deci comutativitatea triunghiului (I.2.1.).

Să presupunem acum că este dată aplicaţia de scindare σ pentru codul (H, α). Luînd $\delta = \gamma\sigma$, triunghiul(I.2.1) este comutativ. Rămîne să mai arătăm că δ este o aplicaţie de decodificare pentru codul (H, α). Avem pentru orice $z \in \Omega(H,\alpha)$, $z = \widehat{\sigma(z)} \in \alpha\gamma\sigma(z) = \alpha\delta(z)$ (v.observaţia I.2.1.). Dacă σ este un homomorfism de scindare, atunci $\delta(z_1z_2) = \gamma\sigma(z_1z_2) = \gamma(\sigma(z_1)\ \sigma(z_2)) = \gamma\sigma(z_1)\gamma\sigma(z_2) = \delta(z_1)\delta(z_2)$, deci δ este un homomorfism de decodificare. De fapt δ este un produs de două homomorfisme. ■

Observaţia I.2.3. Aplicaţiile introduse mai sus se interpretează în procesul de decodificare astfel: să presupunem că este recepţionat un şir admisibil $z \in \Omega(H, \alpha)$. Aplicaţia de scindare distribuie "virgule" între literele lui z, descompunîndu-l pe z în cuvinte din $\alpha(H)$, deci $\sigma(z) \in (\alpha(H))^*$, este o propoziţie pe $\alpha(H)$. Apoi homomorfismul de corectare γ asociază lui $\sigma(z)$ o propoziţie pe H, adică un mesaj din H^*, care conţine pe z în α - domeniul său. Prin aplicaţia de decodificare $\delta = \gamma\sigma$, pentru orice şir admisibil $z \in \Omega(H, \alpha)$, $\delta(z) = \gamma\sigma(z)$ este "versiunea decodificată" al lui z, obţinută prin scindarea mai întîi a propoziţiei admisibile în cuvinte din $\alpha(H)$ (cuvinte în care pot apărea şi erori) şi apoi corectarea cuvintelor din $\alpha(H)$ prin cuvinte - cod din H.

Să ne ocupăm în continuare de alte proprietăţi ale aplicaţiilor introduse.

Observaţia I.2.4. Fie γ un homomorfism de corectare pentru codul (H, α), $\gamma : (\alpha(H))^* \longrightarrow H^*$. Echivalenţa nucleară a acestui homomorfism, $\ker\gamma \subseteq (\alpha(H))^* \times (\alpha(H))^*$ este dată de:

$$\ker\gamma = \{(v_1, v_2) \mid \gamma(v_1) = \gamma(v_2)\}.$$

Scanned with OKEN Scanner

Vom pune $(\alpha(H))^* / \ker \gamma = \{[v]_\gamma \mid v \in (\alpha(H))^*\}$.

Dacă $m, m' \in H^* \subseteq (\alpha(H))^*$ și $m \neq m'$ atunci $[m]_\gamma \cap [m']_\gamma = \emptyset$ deoarece $\gamma(m) = m$. Astfel $(\alpha(H))^*/\ker\gamma = \{[m]_\gamma \mid m \in H^*\}$.

Deoarece $u \rightleftharpoons \gamma(u)$ avem $v \rightleftharpoons m$, $\forall v \in [m]_\gamma$, deci $\ell(v) = \ell(m)$ și $\ell(v(1)) = \ell(m(1)), \ldots, \ell(v(*)) = \ell(m(*))$ și ca atare $\ell(\hat{v}) = \ell(\hat{m})$.

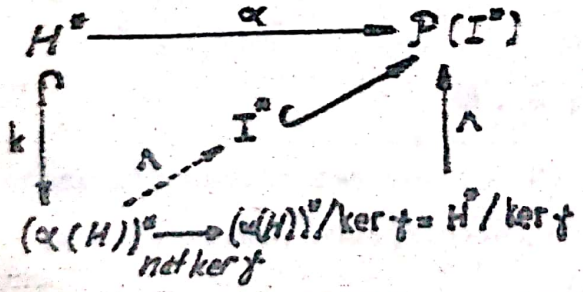
Să notăm $\widehat{[m]}_\gamma \triangleq \{\hat{u} \mid u \in [m]_\gamma\}$, ceea ce realizează definirea aplicației $\wedge : (\alpha(H))^*/\ker\gamma \to P(I^*)$. Are loc

Teorema I.2.3 Pentru orice $m \in H^*$ avem $\alpha(m) = \widehat{[m]}_\gamma$.

Demonstrație. Fie $u \in [m]_\gamma$. Atunci $\gamma(u) = \gamma(m) = m = (p_1, \ldots, p_k)$. Dar $\gamma(u) = \gamma((u_1, \ldots, u_k)) = (p_1, \ldots, p_k)$ cu $u_j \in \alpha(p_j)$, $j = \overline{1,k}$. De aici $\hat{u} = u_1 \ldots u_k \in \alpha(p_1) \ldots \alpha(p_k) = \alpha((p_1, \ldots, p_k)) = \alpha(m)$.

Invers, fie $\hat{u} \in \alpha(m)$ cu $m = (p_1, \ldots, p_k)$. Atunci u se poate scrie sub forma $u = (u_1, \ldots, u_k)$ cu $u_j \in \alpha(p_j)$, $j = \overline{1,k}$. Avem $\gamma(u) = \gamma((u_1, \ldots, u_k)) = (p_1, \ldots, p_k) = m = \gamma(m)$, adică $u \in [m]_\gamma$. ■

Observația I.2.5. Rezultatul obținut în teorema I.2.3 revine la comutativitatea diagramei:



în care k este aplicația de incluziune, iar nat ker γ aplică un element din $(\alpha(H))^*$ pe clasa din $(\alpha(H))^*/\ker\gamma$ căreia îi aparține.

Observația I.2.6. Aplicația de admisibilitate α este separabilă[1] dacă și numai dacă aplicația $\wedge : H^*/\ker\gamma \to P(I^*)$ este separabilă.

1) O aplicație $f : A \to P(B)$ este separabilă dacă din $a_1 \neq a_2$ urmează $f(a_1) \cap f(a_2) = \emptyset$.

Aplicaţia $\wedge : H^*/\ker\gamma \to \mathcal{P}(I^*)$ este separabilă dacă şi numai dacă este injectivă. Intr-adevăr, $\widehat{[m_1]}_\gamma \cap \widehat{[m_2]}_\gamma \neq \emptyset$ dacă şi numai dacă $[m_1]_\gamma \cap [m_2]_\gamma \neq \emptyset$ ceea ce are loc dacă şi numai dacă $[m_1]_\gamma = [m_2]_\gamma$

Aplicaţia $\wedge : H^*/\ker\gamma \to \mathcal{P}(I^*)$ este separabilă dacă aplicaţia $\wedge : (\alpha(H))^* \longrightarrow I^*$ este injectivă.

Intr-adevăr să presupunem că $\wedge : (\alpha(H))^* \to I^*$ este injectivă şi fie $\widehat{[m_1]}_\gamma \cap \widehat{[m_2]}_\gamma \neq \emptyset$. Există atunci $v_1 \in [m_1]_\gamma$, $v_2 \in [m_2]_\gamma$ astfel ca $\hat{v}_1 = \hat{v}_2$ de unde $v_1 = v_2$. Astfel clasele $[m_1]_\gamma$ şi $[m_2]_\gamma$ sînt egale avînd un element v_1 comun.

<u>Consecinţa I.2.1.</u> Aplicaţia de admisibilitate α este separabilă dacă aplicaţia $\wedge : (\alpha(H))^* \to I^*$ este injectivă.

<u>Teorema I.2.4.</u> Fie δ un homomorfism de decodificare pentru codul (H, α) şi $m \in H^*$. Dacă $z \in \alpha(m)$, atunci $m \rightleftharpoons m_1 = \delta(z)$.

<u>Demonstraţie</u>. Fie $m = (p_1, \ldots, p_k) \in H^*$, atunci $z = z_k \ldots z_k$ cu $z_j \in \alpha(p_j)$, $j = \overline{1,k}$. Dacă notăm $\delta(z_j) = r_j$, $j = \overline{1,k}$, atunci $\delta(z) = m_1 = \delta(z_1 \ldots z_k) = \delta(z_1) \ldots \delta(z_k) = r_1 \ldots r_k$. Deoarece δ este un homomorfism de decodificare pentru codul (H, α) avem $z_j \in \alpha\delta(z_j) = \alpha(r_j)$ deci $\ell(z_j) = \ell(\hat{r}_j)$ (v.condiţia ii) din definiţia I.1.1.). Din $z_j \in \alpha(p_j)$, urmează $\ell(p_j) = \ell(z_j) = \ell(\hat{r}_j)$, $j = \overline{1,k}$, deci $m \rightleftharpoons m_1$. ■

Pentru codurile simple (H, ι) teorema precedentă arată că dacă δ este un homomorfism de decodificare pentru (H, ι), atunci $\forall\, m \in H^*$, avem $m \rightleftharpoons \delta(\hat{m})$.

<u>Teorema I.2.5.</u> Fie $m_1, m_2 \in H^*$. Dacă $m_1 \rightleftharpoons m_2$ şi $\alpha(m_1) \cap \alpha(m_2) \neq \emptyset$, atunci $m_1 = m_2$.

Demonstrație. Dacă $m_1 \rightleftharpoons m_2$, atunci $m_1 = (p_1,\dots,p_k)$, $m_2 = (q_1,\dots,q_k)$ cu $l(p_j) = l(q_j)$, $j = \overline{1,k}$. Avem deci $\alpha(p_1)\dots\alpha(p_k) \cap \alpha(q_1)\dots\alpha(q_k) \neq \emptyset$, de unde $\alpha(p_1) \cap \alpha(q_1) \neq \emptyset$ și $\alpha(p_2)\dots\alpha(p_k) \cap \alpha(q_2)\dots\alpha(q_k) \neq \emptyset$. Din $\alpha(p_1) \cap \alpha(q_1) \neq \emptyset$ urmează $p_1 = q_1$. Se continuă la fel cu $\alpha(p_2)\dots\alpha(p_k) \cap \alpha(q_2)\dots\alpha(q_k) \neq \emptyset$. Se obține $p_j = q_j$, $j = \overline{1,k}$, deci $m_1 = m_2$. ■

Teorema I.2.6. Există cel mult un homomorfism de decodificare pentru un cod (H,α).

Demonstrație. Fie δ_1 și δ_2 două homomorfisme de decodificare pentru codul (H,α) și $z \in \Omega(H,\alpha)$. Atunci $z \in \alpha\delta_1(z)$ și $z \in \alpha\delta_2(z)$ și deci $\delta_1(z) \rightleftharpoons \delta_2(z)$ și $\delta_2(z) \rightleftharpoons \delta_1(z)$ (v. teorema I.2.4.). Avem deci $\delta_1(z) \rightleftharpoons \delta_2(z)$ și deoarece $z \in \alpha\delta_1(z) \cap \alpha\delta_2(z)$, urmează în baza teoremei precedente $\delta_1(z) = \delta_2(z)$. ■

Următorul exemplu arată că pentru un cod (H,α) pot exista mai multe aplicații de decodificare.

Exemplul I.2.1. Fie $I = \{0,1\}$, $H = \{01, 10, 0110\}$ și $\alpha = l$. Putem considera aplicațiile de decodificare $\delta_1, \delta_2 : \hat{H}^* \longrightarrow H^*$ care să difere cel puțin pentru propoziția admisibilă $0110 \in \hat{H}^*$. Astfel $\delta_1(0110) = 0110$ și $\delta_2(0110) = (01)(10)$.

Teorema I.2.7. Dacă există un homomorfism de decodificare δ pentru codul (H,α), atunci $\delta(z)$ este unica propoziție din H^* cu proprietatea $m \rightleftharpoons \delta(z)$, pentru $\forall m \in H^*$ cu $z \in \alpha(m)$.

Demonstrație. Să observăm mai întîi că în virtutea teoremei I.2.4, pentru orice $m \in H^*$ cu $z \in \alpha(m)$, avem $m \rightleftharpoons \delta(z)$. Să arătăm că $\delta(z)$ este unica propoziție cu această proprietate. Să presupunem că ar mai exista o propoziție $m_1 \in H^*$ cu $z \in \alpha(m_1)$ și $m \rightleftharpoons m_1$, pentru orice $m \in H^*$ cu $z \in \alpha(m)$. Cum $z \in \alpha\delta(z)$, urmează $\delta(z) \rightleftharpoons m_1$, iar din $z \in \alpha(m_1)$ avem, în baza teoremei I.2.4, $m_1 \rightleftharpoons \delta(z)$.

Deci $m_1 \models \delta(z)$ şi $z \in \alpha(m_1) \cap \alpha\delta(z)$, de unde conform teoremei I.2.5, rezultă $m_1 = \delta(z)$. □

Observaţia I.2.7. Dacă există un homomorfism de decodificare δ pentru codul (H, α), atunci pentru determinarea lui δ este suficientă cunoaşterea lui δ pe o mulţime de generatori a semigrupului $\Omega(H, \alpha)$, lucru foarte important atunci cînd $\Omega(H, \alpha)$ posedă o mulţime finită de generatori.

Se ştie că $\Omega(H,\alpha) = S(\alpha(H))$ (v.teorema I.1.1.), deci $\alpha(H)$ este o mulţime de generatori pentru $\Omega(H,\alpha)$. In cele ce urmează vom pune în evidenţă o submulţime a lui $\alpha(H)$, care de asemenea generează pe $\Omega(H,\alpha)$.

Pot exista în $\alpha(H)$ cuvinte care nu sînt produse de două sau mai multe elemente din $\alpha(H)$. Fie Ω_0 submulţimea lui $\alpha(H)$, formată din totalitatea cuvintelor cu această proprietate.

Are loc

Teorema I.2.8. Avem $\Omega(H,\alpha) = S(\Omega_0)$ şi Ω_0 este unica mulţime minimală de generatori a lui $\Omega(H,\alpha)$, conţinută în $\alpha(H)$.

Demonstraţie. Vom arăta că $\alpha(H) \subseteq S(\Omega_0)$. Fie deci $v \in \alpha(H)$. Dacă $v \in \Omega_0$, atunci $v \in S(\Omega_0)$. Dacă $v \notin \Omega_0$, atunci $v \in (\alpha(H))^j$. Fie $k = \max \{ j \mid v \in (\alpha(H))^j \}$. Avem $v = v_1 \dots v_k$ şi $v_h \in \Omega_0$, $h \in \overline{1,k}$, deoarece în caz contrar ar exista un v_m, $1 \leq m \leq k$ astfel încît $v_m = v'_m v''_m$ şi am avea $v \in (\alpha(H))^{k+1}$, ceea ce contrazice alegerea lui k.

Prin urmare $\Omega(H,\alpha) = S(\alpha(H)) \subseteq S(\Omega_0)$ şi cum $S(\Omega_0) \subseteq S(\alpha(H))$, deoarece $\Omega_0 \subseteq \alpha(H)$, avem $\Omega(H,\alpha) = S(\Omega_0)$.

Să observăm apoi că Ω_0 este o mulţime minimală de gene-

-tori pentru $\Omega(H,\alpha)$. Fie $v \in \Omega_0$ și $\Omega_1 = \Omega_0 \setminus \{v\}$. Avem $S(\Omega_1) \subset \subset \Omega(H,\alpha)$, deoarece $v \in \Omega(H,\alpha)$ și $v \notin S(\Omega_1)$, întrucît în caz contrar am avea $v = v_1 \dots v_m$ cu $v_j \in \Omega_0 \subseteq \alpha(H)$ ceea ce contrazice definiția lui Ω_0 .

Fie acum $G \subseteq \alpha(H)$ o mulțime oarecare de generatori pentru $\Omega(H,\alpha)$, deci $\Omega(H,\alpha) = S(G)$. Vom arăta că $\Omega_0 \subseteq G$. Fie $v \in \Omega_0$. Atunci $v \in S(G) = \Omega(H,\alpha)$. Dacă $v \in G$, atunci $v = v_1' \dots v_m'$ cu $v_k' \in G \subseteq \alpha(H)$, $k = \overline{1,m}$, ceea ce contrazice definiția lui Ω_0 . ■

Observația I.2.8. Pentru orice $v \in \alpha(H)$ există un cuvînt p unic, $p \in H$ cu $v \in \alpha(p)$. Dacă $v \in \alpha(H) \setminus \Omega_0$ atunci există $m \in H^* \setminus H$ cu $v \in \alpha(m)$, cum rezultă din construcția mulțimii Ω_0 .

Teorema I.2.9. Fie δ_1 și δ_2 două aplicații de decodificare pentru codul (H,α). Atunci

1) $\delta_1(\Omega_0) \subseteq H$,

2) $\delta_1(u) = \delta_2(u)$, $\forall u \in \Omega_0$.

Demonstrație. Proprietatea 1) rezultă din alegerea lui Ω_0 . In adevăr, dacă pentru $u \in \Omega_0$, $\delta_1(u) \in H^* \setminus H$, atunci $\delta_1(u) = m$, cu $\ell(m) \geq 2$, deci $m = m_1 m_2$, cu $m_1, m_2 \in H^*$. Cum $u \in \alpha\delta_1(u) = \alpha(m) = \alpha(m_1)\alpha(m_2)$, u ar fi un produs de elemente din $\alpha(H)$, ceea ce contrazice alegerea lui Ω_0 . Prin urmare $\forall u \in \Omega_0$, $\delta_1(u) \in H$.

Cum $u \in \alpha\delta_1(u) \cap \alpha\delta_2(u)$ și $\delta_1(u)$, $\delta_2(u) \in H$, urmează în baza proprietății iii) din definiția I.1.1. că $\delta_1(u) = \delta_2(u)$, deci are loc proprietatea 2). ■

Observația I.2.9. Dacă $v \in \alpha(H) \setminus \Omega_0$, atunci există aplicații de decodificare δ_1 și δ_2 pentru codul (H,α) cu $\delta_1(v) \neq \delta_2(v)$. In adevăr, dacă $v \in \alpha(H) \setminus \Omega_0$, există un cuvînt - cod unic $p \in H$, cu $v \in \alpha(p)$ - deoarece $v \in \alpha(H)$ - și un

mesaj $m \in H^* \setminus H$ cu $v \in \alpha(m)$, deoarece $v \in \alpha(H) \setminus \Omega_0$. Să considerăm aplicaţiile de decodificare δ_1 şi δ_2 pentru codul (H, α) cu $\delta_1(v) = p$, $\delta_2(v) = m$ şi deci $\delta_1(v) \neq \delta_2(v)$.

Prin urmare Ω_0 este submulţimea maximală a lui $\alpha(H)$ pe care toate aplicaţiile de decodificare coincid.

§ I.3. Clase speciale de coduri

In acest paragraf vom introduce coduri care se bucură de anumite proprietăţi extensibile.

Definiţia I.3.1. Un cod corector este un cod (H, α) pentru care dacă $m_1, m_2 \in H^*$ şi $\alpha(m_1) \cap \alpha(m_2) \neq \emptyset$, atunci $m_1 = m_2$.

Observaţia I.3.1. Dacă $\alpha = \iota$, atunci $\alpha(m_1) = \hat{m}_1$ şi un cod simplu (H, ι) este corector dacă, $m_1, m_2 \in H^*$, $m_1 = (p_1, \ldots, p_n)$, $m_2 = (q_1, \ldots q_r)$ şi $\hat{m}_1 = \hat{m}_2$, adică

$$p_1 \cdots p_n = q_1 \cdots q_r$$

atunci $n = r$ şi $p_j = q_j$, $j = \overline{1,n}$.

Această proprietate este cunoscută sub numele de proprietatea de unică descifrabilitate, din care motiv codurile simple corectoare se numesc coduri cu unică descifrabilitate.

In acest caz aplicaţia " $\wedge$ " este bijectivă pe H^*.

Teorema I.3.1. Fie (H, α) un cod. Următoarele afirmaţii sînt echivalente:

C1) Codul (H, α) este corector.

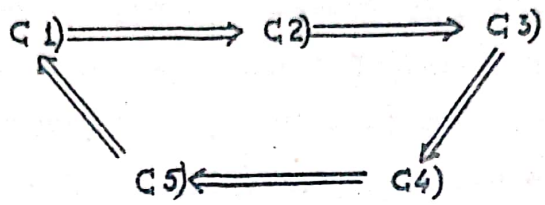
C2) Codul $(\alpha(H)), \iota)$ este unic descifrabil.

C3) Există o singură aplicaţie de scindare pentru codul (H, α).

C4) Există o sihgură aplicaţie de decodificare pentru codul (H, α).

C5)Există un homomorfism de decodificare δ pentru codul (H,α), astfel încît dacă $m \in H^*$ şi $z \in \alpha(m)$, atunci $m = \delta(z)$.

Demonstraţie. Vom arăta următoarele implicaţii:



C1) $\Longrightarrow$ C2). Să presupunem că nu are loc C2).Atunci există $z \in \Omega(H,\alpha)$ şi $m_1, m_2 \in H^*$, astfel încît $z = \hat{m}_1 = \hat{m}_2$ şi $m_1 \neq m_2$.

Atunci $z \in \alpha\gamma(m_1) \cap \alpha\gamma(m_2) \neq \emptyset$ (v.observaţia I,2.1) şi $\gamma(m_1) \neq \gamma(m_2)$. Dacă $\gamma(m_1) = \gamma(m_2)$, atunci cum $m_1 \models \gamma(m_1)$ şi $m_2 \models \gamma(m_2)$, ar urma $m_1 \models m_2$ şi deoarece $\hat{m}_1 = \hat{m}_2$, avem şi $m_1 = m_2$, contrar presupunerii. Deci nu era loc afirmaţia C1).

C2) $\Longrightarrow$ C3) este imediată.

C3) $\Longrightarrow$ C4) urmează din teorema I.2.2.

C4) $\Longrightarrow$ C5) să observăm mai întîi că aplicaţia de decodificare δ (care există în mod unic) este un homomorfism, Din $v \in \alpha\delta(v)$ şi $u \in \alpha\delta(u)$ avem $vu \in \alpha\delta(v)\alpha\delta(u) = \alpha(\delta(v)\delta(u))$. Apoi $vu \in \alpha\delta(vu)$, deci în baza unicităţii aplicaţiei de decodificare avem $\delta(vu) = \delta(v)\delta(u)$. Fie acum $z \in \alpha(m)$ şi $z = z_1 \ldots z_r$ cu $z_j \in \Omega_0$.

Atunci $\delta(z_j) = p_j \in H$, şi $z_j \in \alpha(p_j)$, $j = \overline{1,r}$, de unde $m = (p_1,\ldots,p_r) = \delta(z_1)\ldots\delta(z_r) = \delta(z)$.

C5) $\Longrightarrow$ C1). Fie $\alpha(m_1) \cap \alpha(m_2) \neq \emptyset$, atunci există $z \in \Omega(H,\alpha)$ cu $z \in \alpha(m_1)$ şi $z \in \alpha(m_2)$. Atunci în baza lui C5) $m_1 = \delta(z) = m_2$. ■

Observaţia I.3.2. Din echivalenţa C1)$\Longleftrightarrow$C2), rezultă că proprietatea unui cod de a fi corector este o proprietate extensibilă.

Definiţia I.3.2. Un cod decodabil (cu întîrziere mărginită) este un cod (H, α) pentru care există $n \in N^{*1)}$, astfel încît dacă $\ell(\hat{m}) \geq n$, şi $\alpha(m)I^* \cap \alpha(m_1) \neq \emptyset$, $m, m_1 \in H^*$, atunci $m(1) = m_1(1)$. Cel mai mic număr natural n, pentru care codul (H, α) este decodabil se numeşte întîrzierea codului. Îl vom nota cu n_d.

Observaţia I.3.3. Pentru un cod simplu (H, ι) decodabil, există $n \in N^*$, astfel încît dacă $m_1, m_2 \in H^*$ şi $\hat{m}_1$ şi $\hat{m}_2$ au în comun primii n simboli, atunci mesajele m_1 şi m_2 au primul cuvînt comun, prin urmare pentru mesajele de lungime cel puţin n, primul cuvînt este unic determinat.

Observaţia I.3.4. Dacă printr-un canal de transmitere a informaţiei circulă cuvintele unui cod decodabil cu întîrziere n_d, atunci la recepţionarea unei propoziţii admisibile, identificarea primului ei cuvînt se poate face după transmiterea primilor n_d simboli, deci cu o întîrziere de n_d tacte faţă de începutul transmiterii, ceea ce justifică şi denumirea de cod cu întîrziere mărginită, folosită pentru această clasă de coduri.

Teorema I.3.2. Proprietatea unui cod de a fi decodabil este o proprietate extensibilă.

Demonstraţie. Vom arăta că (H, α) este un cod decodabil dacă şi numai dacă codul extins $(\alpha(H), \iota)$ este decodabil. Fie (H, α) un cod decodabil şi $v, v_1 \in (\alpha(H))^*$ cu $\ell(\hat{v}) \geq n$ şi $\iota(v)I^* \cap \iota(v_1) \neq \emptyset$ adică $\hat{v}.I^* \cap \hat{v}_1 \neq \emptyset$. Fie $m, m_1 \in H^*$ cu $v \in [m]_\gamma$ şi $v_1 \in [m_1]_\gamma$, adică $\gamma(v) = \gamma(m) = m$ şi $\gamma(v_1) = \gamma(m_1) = m_1$. Conform

1) Am notat prin $N^* = \{1, 2, \ldots\}$ iar prin $N = \{0, 1, \ldots\}$.

... teorema I.2.3, avem $\alpha(m)\, I^{*} \cap \alpha(m_1) \neq \emptyset$, şi deoarece $\ell(\hat{m}) \geq n$ (v. observaţia I.2.4), avem $m(1) = m_1(1)$. Dar $\ell(v(1)) = \ell(m(1))$ şi $\ell(v_1(1)) = \ell(m_1(1))$ şi deoarece $\hat{v} r = \hat{v}_1$ cu $r \in I^{*}$, urmează $v(1) = v_1(1)$, deci codul $(\alpha(H), \iota)$ este decodabil.

Să presupunem acum că $(\alpha(H), \iota)$ este un cod decodabil şi fie $\alpha(m)\, I^{*} \cap \alpha(m_1) \neq \emptyset$ cu $m, m_1 \in H^{*}$ şi $\ell(\hat{m}) \geq n$. Există atunci $v \in [m]_\gamma$ şi $v_1 \in [m_1]_\gamma$, astfel încît $\iota(v)\, I^{*} \cap \iota(v_1) \neq \emptyset$ şi cum $\ell(\hat{v}) = \ell(\hat{m}) \geq n$, avem $v(1) = v_1(1)$. Dar $\ell(v(1)) \leq \ell(m(1))$ şi $\ell(v_1(1)) = \ell(m_1(1))$, deci $\alpha(m(1)) \cap \alpha(m_1(1)) \neq \emptyset$ şi din proprietatea iii), definiţia I.1.1, urmează $m(1) = m_1(1)$, deci codul (H, α) este decodabil. ■

Teorema I.3.3. Un cod (H, α) decodabil este şi corector.

Demonstraţie. Fie $\alpha(m_1) \cap \alpha(m_2) \neq \emptyset$, cu $m_1, m_2 \in H^{*}$. De aici urmează că $\alpha(m_1 m_1^{n_1}) \cap \alpha(m_2 m_2^{n_1}) \neq \emptyset$, pentru orice $n_i \in N$. Să alegem $n_1 \in N$, astfel încît $\ell(\widehat{m_1^{n_1}}) \geq n_d$. Aplicînd repetat proprietatea de decodabilitate a codului (H, α), obţinem $m_1(1) = m_2(1)$, $m_1(2) = m_2(2)$ etc. deci $m_1 \in \mathrm{Pref}\{m_2\}$. Prin simetrie găsim $m_2 \in \mathrm{Pref}\{m_1\}$, deci $m_1 = m_2$ şi codul (H, α) este corector. ■

Consecinţa I.3.1. Un cod simplu decodabil are proprietatea de unică descifrabilitate.

In teorema următoare este dată o proprietate a codurilor decodabile care poate fi luată drept definiţie pentru această clasă de coduri.

Teorema I.3.4. Un cod (H, α) este decodabil dacă şi numai dacă există $n_1 \in N^{*}$ astfel încît dacă $\ell(v) \geq n_1$, $v u \in \alpha(m_1)$ şi $v w \in \alpha(m_2)$, atunci $m_1(1) = m_2(1)$.

Demonstraţie. Să presupunem că (H, α) este un cod decodabil şi fie $v u \in \alpha(m_1)$, $v w \in \alpha(m_2)$. Vom arăta că poate fi

ales un $n_1 \in N^*$ astfel încît să aibă loc afirmaţia teoremei.

Putem presupune că $\ell(v) \geq \ell_{max} = \max\{\ell(p) \mid p \in H\}$, deoarece dacă $\ell(v) < \ell_{max}$ şi există $p \in H$ cu $\ell(v) = \ell(p)$, atunci am avea $vu \in \alpha(m_1) = \alpha(p_1 m_3) = \alpha(p_1)\,\alpha(m_3)$ şi $vw \in \alpha(m_2) = \alpha(p_2 m_4) = \alpha(p_2)\,\alpha(m_4)$ cu $p_1, p_2 \in H$ şi $v \in \alpha(p_1) \cap \alpha(p_2)$ deci $p_1 = p_2$ şi $m_1(1) = m_2(1)$. Dacă $\ell(v) \neq \ell(p)$, $\forall p \in H$, atunci $v = v_1 v_2$ cu $\ell(v_1) = \ell(p)$, $p \in H$ şi la fel ca mai sus se arată că $m_1(1) = m_2(1)$. Eliminăm cazul $\ell(v) < \ell_{min} = \min\{\ell(p) \mid p \in H\}$.

Fie deci $\ell(v) > \ell_{max}$ şi $m'_1(m'_2)$ cel mai lung prefix al lui $m_1(m_2)$ cu $\ell(\hat{m}'_1) \leq \ell(v)$ ($\ell(\hat{m}'_2) \leq \ell(v)$). Atunci $\ell(\hat{m}'_1)\,\ell_{max} \geq \ell(v)$ şi $\ell(\hat{m}'_2)\,\ell_{max} \geq \ell(v)$ deoarece dacă am avea $\ell(\hat{m}'_1)\,\ell_{max} < \ell(v)$ ar exista un prefix m''_1 al lui m_1, mai lung decît m'_1 şi $\ell(\hat{m}''_1) \leq \ell(v)$ ceea ce contrazice alegerea lui m'_1. Analog, dacă am avea $\ell(\hat{m}'_2)\,\ell_{max} < \ell(v)$.

Avem $v \in \alpha(m'_1)v_1$, $v \in \alpha(m'_2)v_2$ cu $v_1, v_2 \in I^*$. Să presupunem că $\ell(v_1) \leq \ell(v_2)$; atunci $v_2 = v'v_1$ cu $v' \in I^*$.

Avem $v \in \alpha(m'_1)v_1 \cap \alpha(m'_2)v'v_1 \neq \emptyset$ şi deci $\alpha(m'_1) \cap \alpha(m'_2)\,v' \neq \emptyset$.

Să alegem $n_1 = n\,\ell_{max}$, astfel cînd $\ell(v) \geq n_1$; avem $\ell(m'_2) \geq n$, şi deci $m'_1(1) = m'_2(1)$. Dar $m'_1(1) = m_1(1)$ şi $m'_2(1) = m_2(1)$, deci dacă $\ell(v) \geq n_1$, $vu \in \alpha(m_1)$ şi $vw \in \alpha(m_2)$, atunci $m_1(1) = m_2(1)$. Cazul $\ell(v_1) \geq \ell(v_2)$ se tratează la fel.

Să presupunem că are loc afirmaţia din teoremă şi să luăm $n = n_1$. Dacă $\alpha(m) \cap I^* \cap \alpha(m_1) \neq \emptyset$, atunci există $v \in \alpha(m)$, $u \in I^*$ şi $w \in \alpha(m_1)$ cu $vu = w$. Avem deci $ve = v \in \alpha(m)$, $vu = w \in \alpha(m_1)$ şi $\ell(\hat{m}) = \ell(v)$.

Atunci de îndată ce $\ell(v) \geq n_1$, avem $m_1(1) = m_2(1)$. ∎

<u>Definiţia I.3.3.</u> <u>Un cod sincronizabil</u> este un cod (H, α) cu proprietăţile:

1) este corector

2) există $n \in N^*$ astfel încît dacă $r \in I^*$, $\ell(r) \geq n$ și $r\, I^* \cap \Omega(H,\alpha) \neq \emptyset \neq I^* r \cap \Omega(H,\alpha)$, atunci $r \in \Omega(H,\alpha)$.

Cel mai mic număr natural n, pentru care (H,α) este sincronizabil se numește întîrziere de sincronizare a codului. Il vom nota cu n_s.

Observația I.3.5. Un cod simplu (H, ι) este sincronizabil dacă are proprietatea de mică descifrabilitate și dacă există $n \in N^*$ astfel încît dacă $r \in I^*$, $\ell(r) \geq n$ și rr_1, $r_2 r \in \hat{H}^*$, cu $r_1, r_2 \in I^*$, atunci $r \in \hat{H}^*$.

Observația I.3.6. Pentru un cod sincronizabil, în orice propoziție admisibilă suficient de lungă se poate determina începutul unui cuvînt. Dacă în recepție se pierde o parte din mesajul transmis (se mai spune în acest caz că se pierde sincronizarea) atunci este suficient să se recepționeze următorii n_s simboli pentru a se determina începutul unui cuvînt și se reia decodificarea de la acel cuvînt.

Teorema I.3.5. Proprietatea unui cod de a fi sincronizabil este o proprietate extensibilă.

Demonstrație. Afirmația rezultă imediat din definiția I.3.3. In adevăr proprietatea unui cod de a fi corector este o proprietate extensibilă (v. observația I.3.2.), iar proprietatea 2) exprimîndu-se prin mulțimea șirurilor admisibile $\Omega(H,\alpha)$ este o proprietate extensibilă, deoarece $\Omega(H,\alpha) = \Omega(\alpha(H),\iota)$. ■

Consecința I.3.2. Un cod (H,α) este sincronizabil dacă și numai dacă codul extins $(\alpha(H),\iota)$ este sincronizabil.

Următoarea teoremă arată că proprietatea 2) din definiția I.3.3. poate fi înlocuită prin alte proprietăți echivalente. Mai precis are loc

Teorema I.3.6. Fie (H,α) un cod. Următoarele afirmații sînt echivalente:

(1) Există $n \in \mathbb{N}^*$ astfel încît dacă $r \in I^*$, $\ell(r) \geq n$ și $urv \in \Omega(H,\alpha)$, atunci r admite cel puțin o descompunere de forma $r = r_1 r_2$ și dacă $z_1 r z_2 \in \Omega(H,\alpha)$, atunci $z_1 r_1 \in \Omega(H,\alpha)$ sau $z_1 r_1 = e$ și $r_2 z_2 \in \Omega(H,\alpha)$ sau $r_2 z_2 = e$.

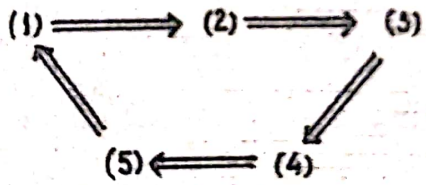
(2) Există $n_1 \in \mathbb{N}^*$, astfel încît dacă $r \in I^*$, $\ell(r) \geq n_1$ și $rI^* \cap \Omega(H,\alpha) \neq \emptyset \neq I^* r \cap \Omega(H,\alpha)$, atunci $r \in \Omega(H,\alpha)$.

(3) Există $n_1 \in \mathbb{N}^*$, astfel încît dacă $r \in I^*$, $\ell(r) \geq n_1$ și $rI^* \cap \alpha(m) \neq \emptyset \neq I^* r \cap \alpha(m)$, cu $m \in H^*$, atunci $r \in \Omega(H,\alpha)$.

(4) Există $n_1 \in \mathbb{N}^*$, astfel încît dacă $r \in I^*$, $\ell(r) \geq n_1$ și $rI^* r \cap \Omega(H,\alpha) \neq \emptyset$ atunci $r \in \Omega(H,\alpha)$.

(5) Există $n_2 \in \mathbb{N}^*$, astfel încît dacă $r \in I^*$, $\ell(r) \geq n_2$ și $t_1 r t_2 \in \Omega(H,\alpha)$ atunci dacă $I^* r \cap \Omega(H,\alpha) \neq \emptyset$, avem $t_1 r \in \Omega(H,\alpha)$, iar dacă $r I^* \cap \Omega(H,\alpha) \neq \emptyset$, avem $r t_2 \in \Omega(H,\alpha)$.

Demonstrație. Vom arăta implicațiile



(1) $\Rightarrow$ (2). Fie $n = n_1$ și să presupunem că $r \in I^*$, $\ell(r) \geq n_1$ și $rs_1 \in \Omega(H,\alpha)$, $s_2 r \in \Omega(H,\alpha)$. In baza afirmației (1) există o descompunere a lui r, $r = r_1 r_2$ și din $r_1(r_2 s_1) \in \Omega(H,\alpha)$ și $(s_2 r_1) r_2 \in \Omega(H,\alpha)$, urmează $r_1 \in \Omega(H,\alpha)$ și $r_2 \in \Omega(H,\alpha)$ deci $r = r_1 r_2 \in \Omega(H,\alpha)$.

(2) $\Rightarrow$ (3) este evidentă.

(3) $\Rightarrow$ (4) Fie $rsr \in \Omega(H,\alpha)$ și $\ell(r) \geq n_1$. Atunci există $m \in H^*$ cu $rsr \in \alpha(m)$, deci $r(sr) \in \alpha(m)$ și $(rs)r \in \alpha(m)$, sau

$r_1 \cap \alpha(m) \neq \emptyset \neq I^* r \cap \alpha(m)$ și în baza afirmației (3) avem $r \in \Omega(H, \alpha)$.

(4) $\Longrightarrow$ (5) Fie $n_2 = n_1 + \ell_{max}$, unde $\ell_{max} = \max\{\ell(p) \mid p \in H\}$ și să presupunem că $t_1 r t_2 \in \Omega(H, \alpha)$ și $I^* r \cap \Omega(H, \alpha) \neq \emptyset$ cu $\ell(r) \geq n_2$. Există $m \in H^*$ cu $t_1 r t_2 \in \alpha(m)$. Fie $m_1 \in Pref\{m\}$ astfel încît $\ell(t_1) \leq \ell(\hat{m}_1) < \ell(t_1) + \ell_{max}$. Atunci $m = m_1 m_2$ și putem să scrim $r = r_1 r_2$ cu $\ell(\hat{m}_1) = \ell(t_1 r_1)$. Avem deci $\ell(r_1) < \ell_{max}$ și $\ell(r_2) \geq n_1$. Este clar că $t_1 r_1 \in \alpha(m_1)$ și $r_2 t_2 \in \alpha(m_2)$. Deoarece există $w \in I^*$, cu $wr \in \Omega(H, \alpha)$, avem $r_2 t_2 w r = r_2 (t_2 w r_1) \cdot r_2 \in \Omega(H, \alpha)$ și $\ell(r_2) > n_1$. Conform cu afirmația (4), avem $r_2 \in \Omega(H, \alpha)$. Dar cum $t_1 r_1 \in \Omega(H, \alpha)$, avem și $t_1 r = t_1 r_1 r_2 \in \Omega(H, \alpha)$.

Fie iar $n_2 = n_1 + \ell_{max}$ și să presupunem că $t_1 r t_2 \in \Omega(H, \alpha)$ și $r I^* \cap \Omega(H, \alpha) \neq \emptyset$ cu $\ell(r) \geq n_2$. Există atunci $m \in H^*$ cu $t_1 r t_2 \in \alpha(m)$. Fie $m_2 \in Suf\{m\}$ astfel încît $\ell(t_2) \leq \ell(\hat{m}_2) < \ell(t_2) + \ell_{max}$. Atunci $m = m_1 m_2$ și putem scrie $r = r_1 r_2$ cu $\ell(\hat{m}_2) = \ell(r_2 t_2)$. Avem deci $\ell(r_2) < \ell_{max}$ și $\ell(r_1) > n_1$. Este clar că $t_1 r_1 \in \alpha(m_1)$ și $r_2 t_2 \in \alpha(m_2)$. Deoarece există $w \in I^*$ cu $rw \in \Omega(H, \alpha)$, avem $rwt_1 r_1 = r_1 (r_2 w t_1) r_1 \in \Omega(H, \alpha)$ și $\ell(r_1) > n_1$. Conform cu afirmația (4), avem $r_1 \in \Omega(H, \alpha)$. Dar cum $r_2 t_2 \in \Omega(H, \alpha)$ avem și $rt_2 = r_1 r_2 t_2 \in \Omega(H, \alpha)$.

(5) $\Longrightarrow$ (1). Să luăm $n = 2n_2 + \ell_{max}$ și să presupunem că $urv \in \Omega(H, \alpha)$ cu $\ell(r) \geq n$. Atunci există $m \in H^*$ cu $urv \in \alpha(m)$. Fie $m_1 \in Pref\{m\}$ astfel încît $\ell(u) + n_2 \leq \ell(\hat{m}_1) < \ell(u) + m_2 + \ell_{max}$ și $r = r_1 r_2$ cu $ur_1 \in \alpha(m_1)$ și $r_2 v \in \alpha(m_2)$, unde $m = m_1 m_2$. Să observăm că $n_2 \leq \ell(r_1) < n_2 + \ell_{max}$ și $n_2 < \ell(r_2)$. Să presupunem acum că $z_1 r z_2 \in \Omega(H, \alpha)$. Atunci avem $z_1 r z_2 = z_1 r_1 (r_2 z_2) \in \Omega(H, \alpha)$ și $ur_1 \in \Omega(H, \alpha)$ cu $\ell(r_1) \geq n_2$, și ținînd seama de afirmația (5) urmează $z_1 r_1 \in \Omega(H, \alpha)$. Apoi $z_1 r z_2 = (z_1 r_1) r_2 z_2 \in \Omega(H, \alpha)$ și cum $r_2 v \in \Omega(H, \alpha)$ cu $\ell(r_2) > n_2$, conform cu (5), avem $r_2 z_2 \in \Omega(H, \alpha)$. ■

Teorema I.3.7. Dacă (H, α) este un cod sincronizabil cu $n_s \leq n$, atunci (H, α) este un cod decodabil cu $n_d \leq n+1$.

Demonstrație. Să presupunem că (H, α) este un cod sincronizabil cu $n_s \leq n$. Vom arăta că (H, α) este un cod decodabil folosind și teorema I.3.4. Fie $v \in I^*$ cu $\ell(v) \geq n+1$ și $vu \in \alpha(m_1)$, $vw \in \alpha(m_2)$, $m_1, m_2 \in H^*$. Vom arăta că $m_1(1) = m_2(1)$. Fie $v = v_1 r$ cu $\ell(r) = n$ și deci $v_1 \neq e$. Codul (H, α) fiind sincronizabil din $v_1 ru \in \alpha(m_1) \subset \Omega(H, \alpha)$ și $\ell(r) = n$, urmează că r admite o descompunere de forma $r = r_1 r_2$ și $v_1 r_1 \in \Omega(H, \alpha)$, $r_2 u \in \Omega(H, \alpha)$. Analog, pornind de la $vw \in \alpha(m_2)$ se obține $r_2 w \in \Omega(H, \alpha)$. Din $r_1 v_1 \in \Omega(H, \alpha)$ urmează existența unui mesaj unic $m \in H^* \setminus \{e\}$ cu $v_1 r_1 \in \alpha(m)$, aceasta deoarece codul (H, α) este și corector. Mesajul m este un prefix al mesajelor m_1 și m_2 și deci $m_1(1) = m(1) = m_2(1)$. Codul (H, α) este decodabil cu $n_d \leq n+1$. ■

Partea II-a

Coduri cu lungime variabilă pentru canale fără zgomot.

Scanned with OKEN Scanner

§ II. 1. Coduri cu unică descifrabilitate

Fie I un alfabet finit cu $|I| \geq 2$, şi I^* semigrupul liber generat de I.

Codul $H \subset I^* \setminus \{e\}$ are proprietatea de unică descifrabilitate, dacă din $\hat{m}_1 = \hat{m}_2$, cu $m_1, m_2 \in H^*$, urmează $m_1 = m_2$, adică din egalitatea:

$$p_1 p_2 \cdots p_n = p'_1 p'_2 \cdots p'_m$$

cu $p_j, p'_k \in H$, $p_j \neq e, p'_k \neq e$, $j = \overline{1,n}$, $k = \overline{1,m}$ urmează $n = m$ şi $p_j = p'_j$, $j = \overline{1,n}$.

Pentru simplitate vom nota "cod cu unică descifrabilitate" prin c.u.d.

Am văzut că un c.u.d este un cod simplu corector (v.definiţia I.3.1.).

Vom prezenta în continuare teoreme de caracterizare a c.u.d. finite.

Teorema II.1.1. Mulţimea finită $H \subset I^*$ este un c.u.d. pe I dacă şi numai dacă există o mulţime nevidă L şi o bijecţie $\varphi : L \longrightarrow H$ care se extinde la un homomorfism injectiv de semigrupuri libere $\varphi : L^* \longrightarrow I^*$.

Demonstraţie. Să presupunem că H este un c.u.d, $H = \{p_1, p_2, \ldots, p_h\}$. Fie $L = \{x_1, x_2, \ldots, x_h\}$ o mulţime finită de simboluri şi $\varphi : L \longrightarrow H$ aplicaţia dată de $\varphi(x_j) = p_j$, $j = \overline{1,h}$. Aplicaţia φ se extinde în mod unic la un homomorfism de semigrupuri $\varphi : L^* \longrightarrow I^*$. Acest homomorfism este injectiv. Într-adevăr, să presupunem că $\varphi(w_1) = \varphi(w_2)$, $w_1 = (x_1, x_2, \ldots, x_n)$, $w_2 = (x'_1, x'_2, \ldots, x'_m)$. De aici $\varphi(x_1)\varphi(x_2)\ldots\varphi(x_n) = \varphi(x'_1)\varphi(x'_2)\ldots\varphi(x'_m)$ şi ţinînd seama de proprietatea de unică

descifrabilitate obţinem $m = n$ şi $\varphi(x_j) = \varphi(x'_j)$, $j = \overline{1,n}$. Cum $\varphi : L \to H$ era o bijecţie avem $x_j = x'_j$, $j = \overline{1,n}$, deci $w_1 = w_2$.

Invers, fie $H \subset I^*$, $H = \{p_1, \ldots, p_h\}$, L o mulţime de simboluri $L = \{x_1, \ldots, x_h\}$ şi $\varphi : L \to H$ bijecţia dată de $\varphi(x_j) = p_j$, $j = \overline{1,h}$. Această bijecţie se extinde la un homomorfism $\varphi : L^* \to I^*$. Să arătăm că din presupunerea că acest homomorfism este injectiv rezultă că H este un c.u.d.

Fie aşadar:

$$p_1 p_2 \ldots p_n = p'_1 p'_2 \ldots p'_m ,$$

cu $p_j, p'_k \in H$, $j = \overline{1,n}$, $k = \overline{1,m}$. Cum φ era o bijecţie putem pune $p_j = \varphi(x_j)$, $p'_k = \varphi(x'_k)$ şi astfel obţinem:

$$\varphi(x_1)\,\varphi(x_2)\ldots\varphi(x_n) = \varphi(x'_1)\,\varphi(x'_2)\ldots\varphi(x'_m)$$

sau

$$\varphi(x_1, \ldots, x_n) = \varphi(x'_1, \ldots, x'_m).$$

Din injectivitatea lui φ găsim $(x_1, \ldots, x_n) = (x'_1, \ldots, x'_m)$, adică $m = n$ şi $x_j = x'_j$, $j = \overline{1,n}$, de unde $p_1 = p'_1, \ldots, p_n = p'_n$. ■

Exemplul II.1.1. Fie $I = \{0,1\}$ şi $H = \{00, 01, 10, 11\}$. H este un c.u.d. Intr-adevăr, fie $L = \{x_1, x_2, x_3, x_4\}$ şi $\varphi : L \to H$ bijecţia dată prin:

x	x_1	x_2	x_3	x_4
$\varphi(x)$	00	01	10	11

Aplicaţia φ se extinde la un homomorfism $\varphi : L^* \to I^*$.

Acest homomorfism este injectiv, aşa cum se poate constata imediat.

Astfel, fie de exemplu $p = 00010111 \in \varphi(L^*) = H^*$. Avem $\varphi^{-1}(p) = x_1 x_2 x_2 x_4$ de unde rezultă că p a fost obţinut din concatenarea cuvintelor 00, 01, 01, şi 11 din H. Astfel s realizează

"descifrarea" cuvîntului p, motiv pentru care φ se mai numeşte homorfism de cifrare.

Teorema II.1.2 . Mulţimea finită $H \subset I^*$ este un c.u.d. pe I dacă şi numai dacă oricare ar fi $u \in I^*$,din $\hat{H}^* u \cap \hat{H}^* \neq \emptyset \neq u\hat{H}^* \cap \hat{H}^*$ rezultă $u \in \hat{H}^*$.

Demonstraţie. Să presupunem că, deşi H satisface condiţia din enunţ, H nu este c.u.d. Există atunci $p_1,\dots,p_n$, $p'_1,\dots p'_m \in H$ astfel încît:

(II.1.1) $\quad p_1 \dots p_n = p'_1 \dots p'_m$

dar $p_1 \neq p'_1$, ceea ce se poate presupune fără a restrînge generalitatea. Astfel $p_1 = p'_1 u$, $u \in I^* \setminus \hat{H}^*$.

Introducînd pe p_1 în egalitatea (II.1.1.) obţinem:

$$u\, p_2 \dots p_n = p'_2 \dots p'_m \in \hat{H}^*.$$

Avem $u \hat{H}^* \cap \hat{H}^* \neq \emptyset$ şi cum $p_1 = p'_1 u$ avem şi $\hat{H}^* u \cap \hat{H}^* \neq \emptyset$. Ca atare, obţinem $u \in \hat{H}^*$, ceea ce este absurd.

Reciproc, să presupunem că H nu satisface condiţia din enunţul teoremei. Vom arăta că H nu este c.u.d.

Există atunci $u \notin \hat{H}^*$ astfel ca $\hat{H}^* u \cap \hat{H}^* \neq \emptyset \neq u\hat{H}^* \cap \hat{H}^*$, adică:

$$p_1 \dots p_n u = p'_1 \dots p'_m, \text{ cu } p_1 \neq p'_1$$

şi

$$u q_1 \dots q_h = q'_1 \dots q'_k,$$

cu $p_1,\dots,p_n, p'_1 \dots p'_m, q_1 \dots, q_h, q'_1,\dots q'_k \in H$.

Atunci $p_1 \dots p_n\, u\, q_1 \dots q_h = p'_1 \dots p'_m q_1 \dots q_h =$
$= p_1 \dots p_n\, q'_1 \dots q'_k$ cu $p_1 \neq p'_1$, deci H nu posedă proprietatea de unică descifrabilitate. ■

Teorema II.1.3. Mulţimea finită $H \subset I^*$ este un c.u.d pe I

dacă şi numai dacă oricare ar fi $u \in I^*$, din

$$u\hat{H}^* \cap \hat{H}^* u \cap \hat{H}^* \neq \emptyset$$

urmează $u \in \hat{H}^*$.

Demonstraţie. Din $u.\hat{H}^* \cap \hat{H}^* u \cap \hat{H}^* \neq \emptyset$ rezultă imediat $u\hat{H}^* \cap \hat{H}^* \neq \emptyset$ şi $\hat{H}^* u \cap \hat{H}^* \neq \emptyset$, deci obţinem condiţia din teorema II.1.2.

Invers, să presupunem că H este un c.u.d.Atunci H satisface condiţiile din teorema precedentă. Atunci $u\, m_1 = m_2$ şi $m_3\, u = m_4$, $m_j \in \hat{H}^*$, $j \in \overline{1,4}$. Urmează $um_1 m_4 = m_2 m_4 = m_2 m_3 u$, deci $m_2 m_4 \in u\hat{H}^* \cap \hat{H}^* u \cap \hat{H}^* \neq \emptyset$. ■

Vom prezenta în continuare o caracterizare laticială a c.u.d., valabilă atît pentru coduri finite cît şi infinite [63].

Fie $P(I^*)$ mulţimea complexelor semigrupului liber I^*. Mulţimea $P(I^*)$ poate fi organizată ca un semigrup faţă de operaţia de înmulţire a complexelor şi anume:

$$\forall K_1, K_2 \in P(I^*),\ K_1K_2 = \{k \mid \exists k_1 \in K_1,\ \exists k_2 \in K_2,\ k = k_1k_2\}.$$

Convenim ca $\emptyset K = K\emptyset = \emptyset$, $\forall K \in P(I^*)$, unde $\emptyset$ este complexul vid.

Avem

$$K_1(K_2 \cup K_3) = K_1K_2 \cup K_1K_3,\quad (K_2 \cup K_3)K_1 = K_2K_1 \cup K_3K_1.$$

Prin urmare, $P(I^*)$ este o latice multiplicativă.

Definiţie.II.1.1.Reziduul la dreapta $K_1 : K_2$, a complexului K_1 prin complexul K_2 este cel mai mare complex R astfel încît

$$RK_2 \subseteq K_1$$

Definiţia II.1.2. Reziduul la stînga, $K_1 :: K_2$, a comple-

xului K_1 prin complexul K_2 este cel mai mare complex L astfel încît

$$K_2 L \subseteq K_1 .$$

Observaţia II.1.1. Pentru oricare două complexe $K_1, K_2 \in P(I^*)$ reziduriile $K_1 : K_2$ şi $K_1 :: K_2$ există totdeauna, deoarece

$$K_1 : K_2 = \bigcup_{HK_2 \subseteq K_1} H ,$$

şi

$$K_1 :: K_2 = \bigcup_{K_2 H \subseteq K_1} H .$$

Observaţia II.1.2. Operaţiile " : " şi" :: " sînt izotone faţa de primul termen şi antiizotone faţă de al doilea termen, deoarece dacă $K_1 \subseteq K$ atunci $K_1 : K_2 \subseteq K : K_2$ şi $K_1 :: K_2 \subseteq K :: K_2$, iar dacă $K \subseteq K_2$ atunci $K_1 : K_2 \subseteq K_1 : K$ şi $K_1 :: K_2 \subseteq K_1 :: K$ cum rezultă imediat din definiţiile II.1.1. şi II.1.2.

Teorema II.1.4. Mulţimea $H \subset I^*$ este c.u.d. pe I, dacă şi numai dacă $\forall K \in P(I^*)$, există $m,n \in N^*$ cu $m \leq n$, astfel încît

(II.1.2) $(H^m : K) \cap H^n \neq \emptyset \neq (\hat{H}^* :: K) \cap \hat{H}^* \Rightarrow K = \{e\}$,

unde $H^m = \{p_1 p_2 \cdots p_m \mid p_j \in H, j = \overline{1,m}\}$.

Demonstraţie. Fie H un c.u.d. pe I şi $K \subset I^*$, astfel încît $(H^m : K) \cap H^n \neq \emptyset \neq (\hat{H}^* :: K) \cap \hat{H}^*$ cu $m,n \in N^*$ şi $m \leq n$. Atunci pentru orice cuvînt $k \in K$, avem ţinînd seama de observaţia I 1.2.

$$H^m : \{k\} \supseteq H^m : K \text{ şi } \hat{H}^* :: \{k\} \supseteq \hat{H}^* :: K,$$

deci

$$(H^m : \{k\}) \cap H^n \neq \emptyset \neq (\hat{H}^* :: \{k\}) \cap \hat{H}^*.$$

Prin urmare

(II.1.3) $p_1 p_2 \cdots p_n k = p'_1 p'_2 \cdots p'_m$, $m \leq n$,

şi

$$(II.1.4)\quad kq_1q_2\cdots q_h = q'_1q'_2\cdots q'_\ell ,$$

cu

$$p_s, p'_t,\ q_u,\ q'_v \in H,\ s=\overline{1,n},\ t=\overline{1,m},\ u=\overline{1,h},\ v=\overline{1,\ell}.$$

Relaţiile (II.1.3) şi (II.1.4) implică

$$p_1p_2\cdots p_nq'_1q'_2\cdots q'_\ell = p'_1p'_2\cdots p'_mq_1q_2\cdots q_h,$$

de unde în baza proprietăţii de unică descifrabilitate, $p_1=p'_1$, $p_2=p'_2,\ldots,q'_\ell = q_h$. Revenind la relaţia (II.1.3) şi simplificînd cu $p_1,\ldots,p_m$ obţinem $p_{m+1}\cdots p_nk = e$, deci $k = e$ şi $K = \{e\}$.

Fie acum $H \subset I^*$, astfel încît pentru orice $K \subset I^*$, să fie satisfăcută condiţia (II.1.2). Vom arăta că H este un c.u.d.

Fie

$$(II.1.5)\quad p_1p_2\cdots p_h = p'_1p'_2\cdots p'_\ell ,$$

cu $p_s, p'_t \in H$, $p_s, p'_t \neq e$, $s = \overline{1,h}$, $t = \overline{1,\ell}$. Dacă $p_1 \neq p'_1$, atunci putem presupune $p_1 = p'_1k$ şi din relaţia (II.1.5) obţinem:

$$kp_2\cdots p_h = p'_2\cdots p'_\ell ,$$

deci $(H : \{k\}) \cap H \neq \emptyset \neq (\hat{H} : \{k\}) \cap \hat{H}^*$, adică are loc condiţia (II.1.2.) cu $m = n = 1$, de unde $k = e$ şi deci $p_1 = p'_1$.

Simplificînd relaţia (II.1.5) cu p_1 obţinem $p_2\cdots p_h = p'_2\cdots p'_\ell$, şi continuăm procedeul. După un număr finit de paşi găsim $h = \ell$ şi $p_j = p'_j$, $j = \overline{1,h}$. ■

Tot cu ajutorul reziduriilor la dreapta şi la stînga se poate obţine o caracterizare a subsemigrupurilor din I^*, care posedă proprietatea de unică descifrabilitate. Astfel are loc :

Teorema II.1.5 [62] .Subsemigrupul $Z \subseteq I^*$ posedă proprietatea de unică descifrabilitate dacă şi numai dacă pentru orice

$\subset I^*$, avem

(II.1.6) $(Z : K) \cap Z \neq \emptyset \neq (Z :: K) \cap Z \Rightarrow K = \{e\}$.

Demonstrație. Fie Z un subsemigrup cu proprietatea de unică descifrabilitate și $K \subseteq I^*$ cu $(Z : K) \cap Z \neq \emptyset \neq (Z :: K) \cap Z$. Atunci $\forall k \in K$, ținînd seama de observația II.1.2, avem

$$Z : \{k\} \supseteq Z : K \text{ și } Z :: \{k\} \supseteq Z :: K ,$$

prin urmare

$$(Z : \{k\}) \cap Z \neq \emptyset \neq (Z :: \{k\}) \cap Z.$$

Avem deci

(II.1.7) $\qquad p_1 k = p'_1,$

și

(II.1.8) $\qquad k p_2 = p'_2,$

cu $p_1, p'_1, p_2, p'_2 \in Z$. Relațiile (II.1.7) și (II.1.8) implică

$$p'_1 p_2 = p_1 p'_2,$$

de unde în baza proprietății de unică descifrabilitate, $p_1 = p'_1$ și $p_2 = p'_2$. Din relația (II.1.7) sau (II.1.8) se obține atunci $k = e$, și deci $K = \{e\}$.

Fie acum Z un subsemigrup din I^*, pentru care este satisfăcută condiția (II.1.6). Vom arăta că Z posedă proprietatea de unică descifrabilitate. Fie, pentru aceasta

(II.1.9) $\qquad p_1 p_2 \cdots p_n = p'_1 p'_2 \cdots p'_m ,$

cu $p_s, p'_t \in Z, p_s, p'_t \neq e$, $s = \overline{1,n}$, $t = \overline{1,m}$. Dacă $p_1 \neq p'_1$, atunci putem presupune că $p_1 = p'_1 k_1$, și din relația (II.1.9) obținem

$$k_1 p_2 \cdots p_n = p'_2 \cdots p'_m ,$$

prin urmare

$$(Z : \{k_1\}) \cap Z \neq \emptyset = (Z :: \{k_1\}) \cap Z,$$

și deci $\{k_1\} = \{e\}$, adică $k_1 = e$ și $p_1 = p'_1$. Simplificînd relația (II.1.9) cu p_1, obținem

$$p_2 \cdots p_n = p'_2 \cdots p'_m .$$

Dacă $p_2 \neq p'_2$, atunci $p_2 = p'_2 k_2$ şi la fel ca mai sus, obţinem $k_2 = e$, deci $p_2 = p'_2$. Repetînd procedeul, după un număr finit de paşi, găsim $n = m$ şi $p_j = p'_j$, $j = \overline{1,n}$. ■

Observatia II.1.3. Fie Z un subsemigrup din I^*. Dacă $K \subsetneq Z$, atunci

$$Z : K \supsetneq Z \text{ şi } Z :: K \supsetneq Z,$$

prin urmare,

(II.1.1o) $Z = (Z:K) \cap Z \supset \emptyset \subset (Z :: K) \cap Z = Z$.

Dacă subsemigrupul Z are proprietatea de unică descifrabilitate, atunci singurul complex $K \subset Z$, cu proprietatea (II.1.1o) este complexul $K = \{e\}$.

§ II.2. Teoremele lui Sardinas-Patterson şi Levenştein de unică descifrabilitate.

Fie I un alfabet finit şi I^* semigrupul liber generat de I. Vom introduce o operaţie parţială pe I^*, prin

Definiţia II.2.1. Cîtul cuvintelor $p, q \in I^*$ este cuvîntul

$$p|q = \begin{cases} r, \text{dacă } p = qr \text{ sau } q = pr \text{ şi } r \neq e, \\ \text{nedefinit, în caz contrar.} \end{cases}$$

Exemplul II.2.1. Fie $I = \{0,1\}$, $p = 010110111$, şi $q = 01011$. Atunci $r = p|q = 0111$.

Observatia II.2.1. Dacă $\ell(p) = \ell(q)$ atunci $p|q$ nu-i definit.

Operaţia "|" este comutativă, $p|q = q|p$, dar nu-i asociativă.

Dacă $p|q = r$, atunci $p \in \mathrm{Pref}_p \{q\}$ sau $q \in \mathrm{Pref}_p \{p\}$. In acest caz $\ell(p) \neq \ell(q)$.

Definitia II.2.2. Cîtul complexelor E_1, $E_2 \subset I^*$ este complexul

$$E_1 | E_2 = \{p|q \mid p \in E_1, q \in E_2\}.$$

Dacă $\forall p \in E_1$, $q \in E_2$ $p|q$ nu-i definit atunci punem $E_1|E_2 = \emptyset$.

In particular dacă $\ell(p) = \ell(q)$, atunci $\{p\}|\{q\} = \emptyset$.

Dacă $r \in E_1|E_2$, atunci $r \in \text{Suf } E_1$ sau $r \in \text{Suf } E_2$, adică $E_1|E_2 \subseteq \text{Suf } E_1 \cup \text{Suf } E_2$. Avem $E_1|E_2 = E_2|E_1$.

Exemplul II.2.2. Fie $I = \{0,1\}$, $E_1 = \{1,10, 011,0010\}$ și $E_2 = \{0,01,11,00,001\}$. Atunci $E_1|E_2 = \{1,11,010,10,0\}$.

Observația II.2.2. Dacă complexele E_1 și E_2 sînt mulțimi uniforme adică $\forall p_1,p_2 \in E_1$, $\ell(p_1) = \ell(p_2)$ și $\forall q_1,q_2 \in E_2$, $\ell(q_1) = \ell(q_2)$, și $E_1|E_2 \neq \emptyset$, atunci $E_1|E_2$ este tot o mulțime uniformă.

Definiția II.2.3. Complexul rezidual al complexului $E \subset I^*$, este cel mai mic complex $R(E) \subset I^*$ cu $E \subseteq R(E)$ și pentru care

$$r \in R(E),\ p \in E \Rightarrow r|p \in R(E).$$

Observația II.2.3. Dat un complex $E \subseteq I^*$ există cel puțin un complex $H \subseteq I^*$, cu $E \subseteq H$ și:

$$\forall r \in H,\ p \in E \Rightarrow r|p \in H,$$

deoarece, cel puțin I^* satisface aceste condiții. Fie $\mathcal{M}(E)$ mulțimea nevidă a complexelor avînd proprietățile de mai sus. Atunci

$$R(E) = \bigcap_{H \in \mathcal{M}(E)} H .$$

Definiția II.2.4. Complexul rezidual al complexului F în raport cu complexul E_2; E_1, $E_2 \in P(I^*)$ este cel mai mic complex $R(E_1,E_2)$ care-l conține pe E_2 și pentru care:

$$r \in R(E_1,E_2),\ p \in E_1 \Rightarrow r|p \in R(E_1,E_2).$$

Observația II.2.4. Date complexele $E_1, E_2 \subset I^*$ există cel puțin un complex $H \subseteq I^*$ cu $E_2 \subseteq H$ și

$$\forall r \in H,\ p \in E_1 \Rightarrow r|p \in H,$$

deoarece I^* satisface aceste condiţii. Prin urmare

$$R(E_1,E_2) = \overbrace{\qquad}^{H \in \mathcal{M}(E_1,E_2)} H,$$

unde am notat prin $\mathcal{M}(E_1,E_2)$ mulţimea nevidă a complexelor care satisfac condiţiile de mai sus.

Observaţia II.2.5. Avem evident $R(E)=R(E,E)$.

Pornind de la două complexe $E_1,E_2 \subset I^*$, vom defini recursiv un şir de complexe reziduale, astfel:

$$R_o(E_1,E_2) = E_2,$$
$$R_1(E_1,E_2) = \{r \mid r \in I^*,\ r = p|q,\ p \in E_2,\ q \in E_1\},$$
$$R_{n+1}(E_1,E_2) = \{r \mid r \in I^*, r = p_n|q,\ p_n \in R_n(E_1,E_2),\ q \in E_1\}.$$

Este clar că $R_n(E_1,E_2)=R_1(E_1,R_{n-1}(E_1,E_2))$ şi că

$R_1(E_1,E_2)=E_2|E_1$, $R_2(E_1,E_2)=(E_2|E_1)|E_1$ etc.

Observaţia II.2.6. Dacă $R_n(E_1,E_2)=\emptyset$, atunci $R_{n+k}(E_1,E_2) = \emptyset$, $\forall k \in N$.

Exemplul II.2.3. Fie $E_1 = \{10,101,001,0111\}$ şi $E_2 = \{0, 1,01,11,111\}$. Atunci obţinem tabloul:

$R_o(E_1,E_2)$	$R_1(E_1,E_2)$	$R_2(E_1,E_2)$	$R_3(E_1,E_2)$	$R_4(E_1,E_2)$
0	01	11	11	
1	111	01		
01	0	111		
11	11			
111				

In cazul particular $E_1=E_2=E$ vom nota prin $R_n(E) = R_n(E,E) = R_1(E, R_{n-1}(E))$.

Exemplul II.2.4. Fie $I = \{0,1\}$ şi $E = \{10,101,001,0111\}$. Atunci obţinem tabloul:

$R_0(E)=E$	$R_1(E)$	$R_2(E)$	$R_3(E)$	$R_4(E)$	$R_5(E)$
10	1	0	01	11	
101		01	111		
001			11		
0111					

Mulţimile $R_n(E_1,E_2)$ au fost considerate pentru prima oară de V.I.Levenştein în 1961 în [36] şi reluate de J.A.Riley în 1967 în [64] .In cazul $E_1 = E_2 = E$ se obţin mulţimile notate cu $Seg_n(E)$ introduse în articolul original al lui A.A.Sardinas şi G.W.Patterson în 1953 [66].

Teorema II.2.1. Are loc:

$$R(E_1,E_2) = \bigcup_{n \in N} R_n(E_1,E_2).$$

Demonstraţie. Să observăm că complexul $H = \bigcup_{n \in N} R_n(E_1,E_2)$ aparţine lui $\mathcal{M}(E_1,E_2)$, prin urmare $R(E_1,E_2) \subseteq H$. Pe de altă parte, fie $r \in R_n(E_1,E_2)$. Vpm arăta prin inducţie după n că $r \in R(E_1,E_2)$.

Dacă $n = 0$, avem $r \in R_0(E_1,E_2) = E_2$ şi, deoarece $E_2 \subseteq R(E_1,E_2)$ avem $r \in R(E_1,E_2)$.

Să presupunemcă $R_n(E_1,E_2) \subseteq R(E_1,E_2)$ şi fie $r \in R_{n+1}(E_1,E_2)$. Atunci $r = p_n|q$ cu $p_n \in R_n(E_1,E_2)$ şi $q \in E_1$. Din ipoteza inductivă $p_n \in R(E_1,E_2)$ şi în baza definiţiei lui $R(E_1,E_2)$ urmează $r \in R(E_1,E_2)$. ■

Vom adopta în continuare notaţia lui Lukasiewicz care elimină scrierea parantezelor. Astfel expresia

$$(\ldots(((p|q_1)|q_2)|q_3)|\ldots)|q_n$$

se va scrie, renunţînd la paranteze, sub forma:

$$|\ldots|||\ pq_1q_2\ldots q_n$$

Teorema II.2.2. Cuvîntul w aparţine lui $R_n(E_1,E_2)$, $n \geq 1$ dacă şi numai dacă el are forma

$$w = |\ldots|||\ pq_1q_2\ldots q_n,$$

unde $p \in E_2$ şi $q_j \in E_1$, $j = \overline{1,n}$.

Demonstraţie. Vom proceda prin inducţie după n.

Pentru $n = 1$ $w \in R_1(E_1,E_2)$ dacă şi numai dacă $w \in E_2 | E_1$, adică dacă şi numai dacă $w = p|q$, $p \in E_2$, $q \in E_1$, deci în acest caz afirmaţia se verifică.

Presupunem afirmaţia adevărată pentru n şi trecem la n+1. Avem $w \in R_{n+1}(E_1,E_2)$ dacă şi numai dacă $w = p_n|q$ cu $p_n \in R_n(E_1,E_2)$ şi $q \in E_1$. Prin ipoteza inductivă $p_n \in R_n(E_1,E_2)$ dacă şi numai dacă $p_n = |\ldots||\ p'q_1q_2\ldots q_n$ cu $p' \in E_2$ şi $q_j \in E_1$, $j = \overline{1,n}$. Prin urmare $w \in R_{n+1}(E_1,E_2)$ dacă şi numai dacă $w = (|\ldots||\ p'q_1q_2\ \ldots\ q_n) | q$, adică dacă şi numai dacă $w = |\ldots|||\ p'q_1q_2\ \ldots\ q_nq$, cu $p' \in E_2$, $q_j \in E_1$, $j = \overline{1,n}$, $q \in E_1$. ■

In continuare vom da o caracterizare a mulţimilor $R_n(E_1,E_2)$.

Definiţia II.2.5. Egalitatea:

(II.2.1) $$p_1p_2\ldots p_n = p'_1p'_2\ldots p'_m,$$

unde $p_j, p'_h \in I^*$, $j = \overline{1,n}$, $h = \overline{1,m}$ este ireductibilă dacă din $p_k \ldots p_n = p'_s \ldots p'_m$ rezultă $k = s = 1$.

Observaţia II.2.7. Dacă egalitatea (II.2.1) este ireductibilă atunci în particular $p_n \neq p'_m$ şi $\ell(p_n) \neq \ell(p'_m)$.

Exemplul II.2.5. Fie $I = \{0,1\}$, $p_1 = 10$, $p_2 = 00$, $p_3 = 11$, $p_4 = 0110$ şi $p'_1 = 100$, $p'_2 = 011$, $p'_3 = 01$, $p'_4 = 10$.

Egalitatea:

$$(10)(00)(11)(0110)=(100)(011)(01)(10),$$

nu este ireductibilă deoarece conţine egalitatea:

$$p_4 = p'_3p'_4,$$

adică

$$0110 = (01)(10).$$

Teorema II.2.3. Fie $\{p_1,\dots,p_n\}$ şi $\{p'_1,\dots,p'_m\}$ două mulţimi de cuvinte din I* astfel încît $p_1\dots p_n = p'_1\dots p'_m$ este o egalitate ireductibilă. Atunci cel mai scurt dintre cuvintele p_n şi p'_m aparţine lui $R(\{p_1,\dots p_n, p'_1,\dots,p'_m\})$ şi are forma:

$$|\dots||r_1r_2\dots r_k,$$

unde cuvintele r_1 şi r_2 sînt sau p_1, p'_1 sau p'_1,p_1.

Demonstraţie. Vom proceda prin inducţie asupra lui n+m. Dacă m+n = 3 atunci $p_1 = p'_1p'_2$ sau $p_1p_2 = p'_1$. In primul caz $p'_2 = |p_1p'_1$, iar în al doilea caz, $p_2 = |p'_1p_1$ şi propoziţia se verifică.

S-o presupunem adevărată pentru $m+n = \ell \geq 3$ şi fie $p_1\dots p_n = p'_1\dots p'_m$ o egalitate ireductibilă cu $m+n = \ell + 1$.

Dacă n = 1 atunci $p_1 = p'_1\dots p'_m$. De aici $|p_1p'_1 = p'_2\dots p'_m$, apoi $||p_1p'_1p'_2 = p'_3\dots p'_m$ ş.a.m.d., iar în final $|\dots||p_1p'_1\dots p'_{m-1} = p'_m$.

Similar se procedează în cazul m = 1 obţinîndu-se $|\dots||p'_1p_1\dots p_{n-1} = p_n$ şi propoziţia se verifică.

Vom presupune deci $m,n \geq 2$. Avem $p_1 \neq p'_1$, deoarece dacă $p_1 = p'_1$, egalitatea n-ar fi ireductibilă. Să presupunem că $\ell(p_1) < \ell(p'_1)$. Atunci $p'_1 = p_1q_1$ şi găsim:

$$p_2\dots p_n = q_1p'_2\dots p'_m.$$

Această egalitate este ireductibilă deoarece, în caz

contrar ar antrena reductibilitatea egalităţii:

$$p_1p_2\cdots p_n = p'_1p'_2\cdots p'_m.$$

Folosind ipoteza inductivă cel mai scurt dintre cuvintele p_n şi p'_m se scrie sub forma:

$$|\cdots \| q_1\ p_2\cdots$$

şi deoarece $q_1 = |p'_1p_1$ ultima expresie revine la

$$|\cdots \| p'_1p_1p_2\cdots \quad . \blacksquare$$

Teorema II.2.4. [Levenştein [41]]. Cuvîntul nenul w aparţine lui $R_n(E_1,E_2)$, $n \geq 1$ dacă şi numai dacă există $p_0 \in E_2$, $p_1,\ldots,p_n \in E_1$ şi un întreg k, $1 \leq k \leq n$ astfel încît are loc una din următoarele două situaţii:

1) în egalitatea ireductibilă:

$$p_0p_1\cdots p_{k-1}w = p_k\cdots p_n,$$

avem $\ell(w) < \ell(p_n)$,

2) în egalitatea ireductibilă

$$p_0p_1\cdots p_{k-1} = p_k\cdots p_nw,$$

avem $\ell(w) < \ell(p_{k-1})$.

Demonstraţie. Dacă există $p_0,p_1,\ldots,p_n$ astfel încît să aibă loc una din cele două situaţii de mai sus atunci, în baza teoremei II.2.3, $w = |\ \cdots |\ p_0p_k\cdots$ şi conform teoremei II.2.2 $w \in R_n(E_1,E_2)$.

Reciproc, dacă $w \in R_n(E_1,E_2)$ vom demonstra prin inducţie după n că are loc una din condiţiile din enunţul teoremei.

Dacă $n = 1$ atunci $w \in R_1(E_1,E_2)$ şi, sau $pw = q$ sau $qw = p$, $p \in E_2$, $q \in E_1$ şi propoziţia este verificată, egalităţile fiind evident ireductibile.

Presupunem afirmaţia adevărată pentru $n \geq 1$ şi fie $w \in R_{n+1}(E_1,E_2)$. Atunci există $r_n \in R_n(E_1,E_2)$ şi $q \in E_1$ astfel încît sau $r_n = qw$ sau $q = r_nw$. Prin ipoteza inductivă există atunci

$p_0 \in E_2$, $p_1, \dots, p_n \in E_1$ și întregul k cu $p_0p_1 \dots p_{k-1} r_n = p_k \dots p_n$ sau $p_0p_1 \dots p_{k-1} = p_k \dots p_n r_n$, cu $\ell(r_n) < \ell(p_n)$ sau $\ell(r_n) < \ell(p_{k-1})$.

Combinînd cazurile de mai sus rezultă următoarele patru situații posibile:

i) $r_n = qw$ și $p_0 \dots p_{k-1} r_n = p_k \dots p_n$,

ii) $r_n = qw$ și $p_0p_1 \dots p_{k-1} = p_k \dots p_n r_n$,

iii) $r_n w = q$ și $p_0 \dots p_{k-1} r_n = p_k \dots p_n$,

iv) $r_n w = q$ și $p_0p_1 \dots p_{k-1} = p_k \dots p_n r_n$,

de unde obținem egalitățile ireductibile,

i') $p_0 \dots p_{k-1} qw = p_k \dots p_n$,

ii') $p_0 \dots p_{k-1} = p_k \dots p_n qw$,

iii') $p_0 \dots p_{k-1} q = p_k \dots p_n w$,

iv') $p_0 \dots p_{k-1} w = p_k \dots p_n q$.

Punînd $q = p_{n+1} \in E_1$, atunci dacă $w \in R_{n+1}(E_1, E_2)$, există $p_0 \in E_2$, $p_1, \dots, p_{n+1} \in E_1$, astfel încît să aibă loc sau (i') sau iii')) sau (ii') sau iv')), adică are loc unul din cele două cazuri din enunț. Să mai observăm că $\ell(w)$ este strict mai mic decît lungimea ultimului cuvînt din membrul în care nu apare w, corespunzător fiecărui caz în parte. ■

Observația II.2.8. Din relațiile din enunțul teoremei precedente rezultă că elementele mulțimii $R_n(E_1, E_2)$ sînt sufixe ale cuvintelor din mulțimea E_1.

Consecința II.2.1. Fie $w \in I^*$ și $E_2 = \{p_0\}$. Există $p_j \in E_1$, $j = \overline{1,n}$ astfel ca $w = |\dots|| p_0q_1q_2 \dots q_n$ dacă și numai dacă există $p_1, \dots, p_n \in E_1$ și un întreg k, $1 \leq k \leq n$ astfel încît are loc una din următoarele două situații:

1) în egalitatea ireductibilă:

(II.2.2.) $$p_0p_1 \dots p_{k-1} w = p_k \dots p_n,$$

avem $\ell(w) < \ell(p_n)$.

2)în egalitatea ireductibilă:

(II.2.3). $$p_0p_1\cdots p_{k-1} = p_k\cdots p_n\, w,$$

avem $\ell(w) < \ell(p_{k-1})$.

Faptul se obţine imediat din teoremele II.2.2. şi II.2.4.

Consecinţa II.2.2. Să presupunem că, în condiţiile consecinţei II.1.1. luăm $w = p_0$. Atunci are loc fie egalitatea (II.2.2.) fie egalitatea (II.2.3.). În primul caz avem $p_0p_1\cdots p_{k-1}p_0 = p_k\cdots p_n$ cu $\ell(p_0) < \ell(p_n)$, de unde înmulţind în ambii membri cu $p_1\cdots p_{k-1}\,p_0$ avem

$$p_0p_1\cdots p_{k-1}p_0p_1\cdots p_{k-1}p_0 = p_k\cdots p_np_1\cdots p_{k-1}p_0\,,$$

sau

$$p_0p_1\cdots p_{k-1}p_k\cdots p_n = p_k\cdots p_np_1\cdots p_{k-1}p_0.$$

Observăm că avem şi $\ell(p_0) < \ell(p_n)$.

În al doilea caz avem egalitatea

$$p_0p_1\cdots p_{k-1} = p_k\cdots p_np_0,$$

cu $\ell(p_0) < \ell(p_{k-1})$.

Cele două cazuri de mai sus pot fi prezentate unitar sub următoarea formă:

Există $q_j \in E_1$, $j = \overline{1,n}$ şi $p_0 \in I^a \setminus \{e\}$, astfel încît $p_0 = |\cdots||p_0q_1\cdots q_n$ dacă şi numai dacă are loc o egalitate de forma

$$p_0r_1\cdots r_t = r'_1\cdots r'_sp_0,$$

cu $\ell(p_0) < \ell(r_t)$, r_j, $r'_h \in E_1$, $j = \overline{1,t}$, $h = \overline{1,s}$, şi $t = s = n$ sau $t + s = n$.

Consideraţiile de mai sus permit o nouă caracterizare pentru coduri cu unică descifrabilitate.

Teorema II.2.5. [Sardinas - Patterson [66].] Mulţimea $H \subseteq I^*$ este un cod cu unică descifrabilitate dacă şi numai dacă $R_n(H) \cap H = \emptyset$, $\forall n \geq 1$.

Demonstraţie. Să presupunem că $R_n(H) \cap H \neq \emptyset$ şi fie $w \in R_n(H) \cap H$. Atunci, aplicînd teorema lui Levenştein cu $E_1 = E_2 = H$ există o egalitate ireductibilă de forma

$$p_0 p_1 \cdots p_{k-1} w = p_k \cdots p_n,$$

cu $p_j \in H$, $j = \overline{0,n}$, $w \in H$ şi $\ell(w) < \ell(p_n)$. Astfel $w \neq p_n$ şi H nu posedă proprietatea de unică descifrabilitate.

Reciproc, dacă H nu este c.u.d. atunci există egalitatea:

$$p_1 p_2 \cdots p_n = p'_1 p'_2 \cdots p'_m,$$

cu $p_j, p'_h \in H$, $j = \overline{1,n}$, $h = \overline{1,m}$, cu $p_n \neq p'_m$. Fie $m+n = k$.

Atunci $k \geq 3$. Putem presupune că egalitatea este ireductibilă, fără a restrînge generalitatea, deoarece în caz contrar prin simplificare ajungem în orice caz la o egalitate ireductibilă. Deoarece $p_n \neq p'_m$ unul din aceste cuvinte este mai scurt, fie el p_n. Atunci, conform teoremei II.2.4. $p_n \in R_{k-2}(H) \cap H$, $k-2 \geq 1$. ■

Observaţia II.2.9. Teorema precedentă oferă un algoritm care ne permite să decidem dacă o mulţime finită $H \subseteq I^*$ este c.u.d.,

Deoarece elementele din $R_n(H)$, $n \geq 1$ sînt sufixe pentru cuvintele din H (v.observaţia II.2.8) şi H este o mulţime finită, atunci $R_n(H) \subseteq \text{Suf } H$ şi Suf H este o mulţime finită. Astfel

$$R(H) = \bigcup_{n \in \mathbb{N}} R_n(H) \subseteq \text{Suf } H,$$

şi R(H) este o mulţime finită. Ca atare mulţimea P(R(H)) este finită şi şirul $R_1(H), R_2(H), \ldots, R_n(H), \ldots$ devine în mod necesar periodic. Există $n_0 \in \mathbb{N}^*$ şi $n_1 \in \mathbb{N}^*$ astfel că, dacă $R_{n_0}(H) \neq \emptyset$ atunci

$R_{n_o}(H) = R_{n_1}(H)$ cu $n_1 < n_o$. Astfel, va fi suficient să verificăm că $R_j(H) \cap H = \emptyset$ pentru $j = \overline{1,n_o}$ pentru a constata că H este un c.u.d. Acest procedeu este cunoscut sub numele de algoritmul lui Sardinas - Patterson.

Observaţia II.2.10. Folosind rezidul la stînga a două complexe (v.definiţia II.1.2) teorema II.2.5 poate fi enunţată sub forma echivalentă:

Teorema II.2.6. Mulţimea $H \subseteq I^*$ este un cod dacă şi numai dacă $[(R_n(H) :: H) \cup (H :: R_n(H))] \cap H = \emptyset, \forall n \geq 1$.

Demonstraţie. Este suficient să observăm că $R_1(H) = H :: H$, iar $R_{n+1}(H) = (R_n(H) :: H) \cup (H :: R_n(H))$. ■

Fie acum E_1, $E_2 \in P(I^*)$ şi $|E_1| < \infty$.

Teorema II.2.7. [Riley [64]] .Dacă există $n \in N$ astfel încît $R_n(E_1,E_2) \subseteq E_2 \cup R_1(E_1,E_2) \cup \ldots \cup R_{n-1}(E_1,E_2)$ atunci

$$\bigcup_{j \in N^*} R_j(E_1,E_2) = \bigcup_{j=1}^{n} R_j(E_1,E_2).$$

Demonstraţie. Să presupunem că există $n \in N^*$ astfel încît $R_n(E_1,E_2) \subseteq E_2 \cup R_1(E_1,E_2) \cup \ldots \cup R_{n-1}(E_1,E_2)$ şi fie $p \in R_{n+1}(E_1,E_2)$. Atunci $p = p' \mid q$, $p' \in R_n(E_1,E_2)$ şi $q \in E_1$. Deoarece $R_n(E_1,E_2) \subseteq E_2 \cup R_1(E_1,E_2) \cup \ldots \cup R_{n-1}(E_1,E_2)$ avem $p' \in E_2$ sau există j cu $1 \leq j \leq n-1$ astfel ca $p' \in R_j(E_1,E_2)$.

In primul caz $p \in R_1(E_1,E_2)$, iar în al doilea $p \in R_{j+1}(E_1,E_2)$, de unde $R_{n+1}(E_1,E_2) \subseteq E_2 \cup R_1(E_1,E_2) \cup \ldots \cup R_{n-1}(E_1,E_2)$. Analog se arată $R_{n+k}(E_1,E_2) \subseteq E_2 \cup R_1(E_1,E_2) \cup \ldots \cup R_{n-1}(E_1,E_2)$, $\forall k \in N$. ■

Teorema II.2.8. [Riley [64]] .Fie $E \subset I^*$, cu $|E| < \infty$ şi t numărul sufixelor proprii ale cuvintelor din E, sufixe care nu aparţin lui E, $t = |SufpE| = |SurE \setminus (E \cup \{e\})|$. Atunci $R(E) =$

$= \bigcup_{j=1}^{t+1} R_j(E)$.

Demonstrație. Să presupunem că $R(E) \neq \bigcup_{j=1}^{t+1} R_j(E)$.

Atunci, în baza teoremei II.2.7, $R_j(E) \not\subseteq E \cup R_1(E) \cup \ldots \cup R_{j-1}(E)$, $j = \overline{1,t+1}$. In particular $R_1(E) \not\subseteq E$ astfel că există $p_1 \in R_1(E)$, $p_1 \notin E$. Similar, există $p_2 \in R_2(E)$, $p_2 \notin E \cup R_1(E)$, ş.a.m.d. Obţinem astfel mulţimea de cuvinte distincte $p_1, \ldots p_{t+1}$, care sînt sufixe proprii ale cuvintelor din E, ceea ce contrazice presupunerea că există numai t sufixe proprii distincte. Deci $R(E) = \bigcup_{j=1}^{t+1} R_j(E)$. ■

Teorema II.2.9. Mulţimea finită $H \subseteq I^*$ este un c.u.d. pe I dacă şi numai dacă $R_j(H) \cap H = \emptyset$, $j = \overline{1,t+1}$, unde $t = |\mathrm{Sufp}\ H|$.

Demonstrație. Afirmaţia rezultă imediat din teorema precedentă şi din observaţia că, dacă există $n \in \mathbb{N}^*$ cu $R_n(H) \cap H \neq \emptyset$ atunci $\left[R_1(H) \cup \ldots \cup R_{t+1}(H)\right] \cap H \neq \emptyset$. ■

Exemplul II.2.6. Fie $I = \{0,1\}$ şi $H = \{10, 00, 01, 11, 0110\}$. Atunci $\mathrm{Suf}\ H \setminus (H \cup \{e\}) = \{0, 1, 110\}$. Deci $|\mathrm{Suf}\ H \setminus (H \cup \{e\})| = 3$. Avem:

$R_0(H)$	$R_1(H)$	$R_2(H)$	$R_3(H)$	$R_4(H)$
10	1	0	0	0
00	10	01	1	1
01		1	110	110
101			10	01
0110			01	10

Prin urmare $R_1(H) \cap H = \{10\}$, $R_2(H) \cap H = \{01\}$, $R_3(H) \cap H = \{10, 01\}$, $R_4(H) \cap H = \{01, 10\}$.

Deoarece $R_j(H) \cap H \neq \emptyset$, $j = \overline{1,4}$, codul H nu are proprie-

tatea de unică descifrabilitate.

Exemplul II.2.7. Fie $I = \{0,1\}$ şi $H = \{1,10,011,0010\}$. Atunci $Suf\ H \setminus (H \cup \{e\}) = \{0,11,010\}$. Deci $|Suf\ H \setminus (H \cup \{e\})| = 3$. Avem:

$R_0(H)$	$R_1(H)$	$R_2(H)$	$R_3(H)$	$R_4(H)$
1	0	11		
10		010		
011				
0010				

Avem $R_3(H) = \emptyset$, deci $R_n(H) = \emptyset$, $n \geq 3$, prin urmare $R_n(H) \cap H = \emptyset$, $n \geq 3$. Apoi $R_1(H) \cap H = \emptyset$ iar $R_2(H) \cap H = \emptyset$. Codul H este unic descifrabil.

Vom prezenta acum demonstraţia elementară a lui G. Bandyopadhay [4]pentru teorema lui Sardinas-Patterson.

Cuvintele din I^* vor fi reprezentate prin segmente pe o dreaptă, lungimea segmentelor fiind proporţională cu lungimea cuvintelor.

Fie egalitatea ireductibilă :

(II.2.4.) $$p_1 p_2 \cdots p_n = p'_1 p'_2 \cdots p'_m,$$

reprezentată în fig.II.2.1, unde p_j, p'_k, $j = \overline{1,n}$, $k = \overline{1,m}$, sînt cuvinte distincte dintr-o mulţime finită de cuvinte $H \subseteq I^* \setminus \{e\}$.

Fie A punctul care marchează începutul segmentelor de pe dreaptă, segmente care reprezintă cei doi membri ai egalităţii (II.2.4.), AA_1 fiind reprezentarea cuvîntului p_1, $A_1 A_2$ reprezentarea cuvîntului p_2 ş.a.m.d., AA'_1 fiind reprezentarea cuvîntului p'_1, $A'_1 A'_2$ reprezentarea cuvîntului p'_2 ş.a.m.d.

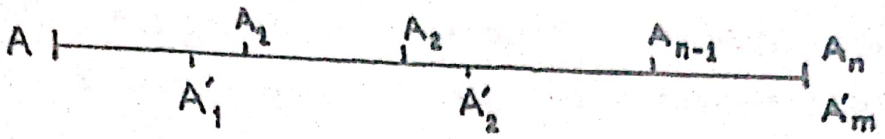


Fig.II.2.1

Deoarece egalitatea (II.2.4.) este ireductibilă numai punctele A_n și A'_m coincid. Să observăm să segmentul A'_1A_1 este imaginea unui cuvînt din $R_1(H)$, deoarece A_1 se află la dreapta lui A'_1. In cazul cînd A_1 ar fi fost la stînga lui A'_1 atunci cuvîntul corespunzător lui $A_1A'_1$ ar fi aparținut lui $R_1(H)$.

Pentru situația reprezentată în fig.II.2.1 segmentul $A_1A'_2$este imaginea unui cuvînt din $R_2(H)$ deoarece cuvintele din $R_2(H)$ se obțin făcînd cîtul cuvintelor din $R_1(H)$ prin cuvinte din H. Se constată că $A_2A'_2$ este imaginea unui cuvînt din $R_3(H)$, ș.a.m.d.

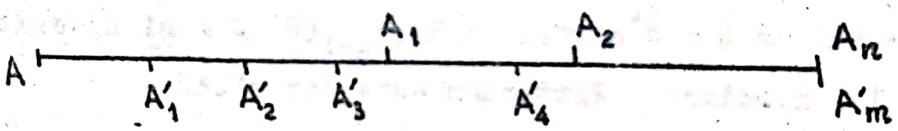


Fig.II.2.2.

In situația reprezentată în fig.II.2.2. A'_1A_1 este imaginea unui cuvînt din $R_1(H)$, A'_2A_1 este imaginea unui cuvînt din $R_2(H)$, A'_3A_1 este imaginea unui cuvînt din $R_3(H)$ și $A_1A'_4$ reprezintă un cuvînt din $R_4(H)$ etc. In general, cuvîntul reprezentat de $A_1A'_r$ aparține lui $R_r(H)$ dacă A'_r este primul dintre punctele A'_h care se află la dreapta lui A_1. Continuînd în același mod se observă că, cuvîntul reprezentat de A'_rA_ℓ aparține lui $R_{r+\ell-1}(H)$, dacă A_ℓ este primul punct A_j aflat la dreapta lui A'_r. In cazul din fig.II.2.2. A'_4A_2 reprezintă un cuvînt din $R_5(H)$. Astfel, fiecare punct din mulțimea $\{A_j, A'_h \mid j = \overline{1,n}, h = \overline{1,m}\}$ reprezintă începutul sau sfîrșitul unui cuvînt care apar -

ţine unei mulţimi $R_r(H)$. Apoi, fiecare cuvînt dintr-o mulţime $R_r(H)$ este reprezentat printr-un segment $A_jA'_h$ sau A'_hA_j, ceea ce se verifică imediat prin inducţie asupra numărului j+h. Astfel, pentru j+h = 2 (am văzut că A'_1A_1 sau $A_1A'_1$ reprezintă cuvinte din $R_1(H)$. Să presupunem acum că A'_rA_ℓ reprezintă un cuvînt din $R_k(H)$ Atunci $A_\ell A'_{r+1}$ sau $A'_{r+1}A_\ell$ reprezintă un cuvînt din $R_{k+1}(H)$, după cum A'_{r+1} se află la dreapta sau la stînga lui A_ℓ .

Fie acum A_{n-1} punctul cel mai apropiat de extremitatea dreaptă comună, marcată cu A_n şi A'_m. Dacă A_{n-1} este sfîrşitul unui segment, care reprezintă un cuvînt din $R_t(H)$ atunci acest segment trebuie să fie $A'_{m-1}A_{n-1}$. Prin urmare segmentul $A_{n-1}A'_m = A_{n-1}A_n$ reprezintă un cuvînt aflat atît în H cît şi în $R_{t+1}(H)$, deci $H \cap R_{t+1}(H) \neq \emptyset$. Analog se procedează dacă cel mai apropiat punct de extremitatea dreaptă ar fi A'_{m-1}.

Astfel, dacă H nu are proprietatea de unică descifrabilitate există $t \in N^*$ astfel ca $H \cap R_{t+1}(H) \neq \emptyset$ şi necesitatea teoremei lui Sardinas - Patterson este dovedită.

Pentru a demonstra suficienţa vom presupune, pentru fixarea ideilor că $H \cap R_3(H) \neq \emptyset$ şi vom arăta că H nu are proprietatea de unică descifrabilitate, construind efectiv o egalitate ireductibilă avînd termenii formaţi din cuvinte distincte din H. Cazul $H \cap R_k(H) \neq \emptyset$ se tratează analog.

Există patru posibilităţi pentru obţinerea unui cuvînt din $H \cap R_3(H)$ pe care le vom ilustra în figura II.2.3., printr-un arbore. In cazul cînd p_k este un prefix al cuvîntului p_ℓ convenim să notăm prin $p_\ell - p_k$ cuvîntul care se obţine îndepărtînd din cuvîntul p_ℓ prefixul p_k.

Vom nota cu s_ℓ^k un cuvînt din mulţimea $R_k(H)$. Aceste patru situaţii pot fi descrise prin ecuaţii folosind convenţia făcută mai sus.

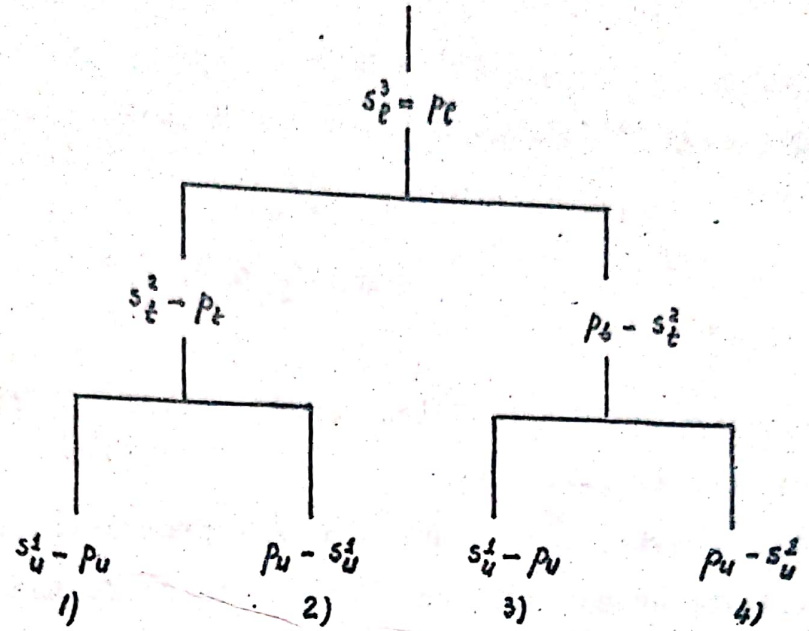


Fig.II.2.3.

Astfel,pentru cazul 1) avem:

$$s_\ell^3 = p_\ell = s_t^2 - p_t \text{ sau } s_t^2 = p_\ell + p_t$$

$$s_t^2 = s_u^1 - p_u \text{ sau } s_u^1 = s_t^2 + p_u$$

$$s_u^1 = p_v - p_z \text{ sau } p_v - p_z = p_\ell + p_t + p_u$$

şi deci $p_v = p_z + p_\ell + p_t + p_u$, de unde egalitatea ireductibilă

$$p_v = p_z p_\ell p_t p_u .$$

Similar se procedează şi în celelalte cazuri obţinîndu-se în fiecare caz cîte o egalitate ireductibilă, ceea ce arată că H nu are proprietatea de unică descifrabilitate.

§ II.3. Unica descifrabilitate infinită si ciclică.

Definiţia II.3.1. Un cod H posedă proprietatea de unică descifrabilitate infinită dacă, din egalitatea:

$p_1 p_2 \cdots = p'_1 p'_2 \cdots$, $p_j p'_k \in H$, $j, h \in \mathbb{N}^*$, rezultă $p_1 = p'_1$.

Definiția II.3.2. Codul H posedă proprietatea de unică descifrabilitate ciclică dacă nu are loc o egalitate de forma:

$$up_1 \dots p_k = p'_1 \dots p'_h u$$

cu $h \geq 1$ și $0 < \ell(u) < \ell(p'_1)$, $p_j, p'_\ell \in H$, $j = \overline{1,k}$, $\ell = \overline{1,h}$, $u \in I^*$.

Observația II.3.1. Unica descifrabilitate infinită implică unica descifrabilitate.

Într-adevăr, dacă codul H nu are proprietatea de unică descifrabilitate atunci are loc o egalitate de forma:

$$p_1 \dots p_k = p'_1 \dots p'_s ,$$

cu $p_1 \neq p'_1$, p_j, $p'_h \in H$, $j = \overline{1,k}$, $h = \overline{1,s}$. Dar atunci are loc egalitatea:

$$p_1 \dots p_k p_k p_k \dots = p'_1 \dots p'_s p_k p_k \dots ,$$

cu $p_1 \neq p'_1$, deci codul H nu posedă nici proprietatea de unică descifrabilitate infinită.

Observația II.3.2. Unica descifrabilitate ciclică implică unica descifrabilitate.

Să presupunem că H nu are proprietatea de unică descifrabilitate.

Există atunci o egalitate ireductibilă:

$$p_1 \dots p_k = p'_1 \dots p'_s , \tag{II.3.1}$$

cu $p_1 \neq p'_1$, p_j, $p'_h \in H$, $j = \overline{1,k}$, $h = \overline{1,s}$. Dacă presupunem $\ell(p_1) < \ell(p'_1)$ atunci putem scrie

$$p'_1 = p_1 u_1 , \quad u_1 \in I^* .$$

De aici, ținînd seama de egalitatea (II.3.1) obținem:

$$u_1 p_2 \dots p_k = p'_2 \dots p'_s ,$$

și deci:

$$u_1 p_2 \dots p_k p'_1 = p'_2 \dots p'_s p_1 u \tag{II.3.2}$$

cu $0 < \ell(u_1) < \ell(p_1)$.

Dacă $\ell(u_1) < \ell(p'_2)$ atunci egalitatea (II.3.2) asigură că H nu posedă proprietatea de unică descifrabilitate ciclică.

Să observăm că $\ell(u_1) \neq \ell(p'_2)$ deoarece în caz contrar am avea $u_1 = p'_2$, de unde ar urma că:

$$p_2 \cdots p_k = p'_3 \cdots p'_s$$

şi egalitatea (II.3.1) ar fi reductibilă.

Rămîne deci $\ell(u_1) > \ell(p'_2)$. Atunci $u_1 = p'_2 u_2$ şi (II.3.2.)conduce la:

$$u_2 p_2 \cdots p_k p'_1 = p'_3 \cdots p'_s p_1 p'_2 u_2$$

cu $0 < \ell(u_2) < \ell(u_1) < \ell(p_1)$.

Dacă $\ell(u_2) < \ell(p'_3)$ codul H nu posedă proprietatea de unică descifrabilitate ciclică.

Dacă $\ell(u_2) > \ell(p'_3)$ aplicăm acelaşi procedeu. Deoarece la pasul j obţinem un cuvînt $u_j \in X^*$ cu $0 < \ell(u_j) < \ell(u_{j-1})$ procedeul se termină după un număr finit de paşi obţinînd o egalitate care neagă proprietatea de unică descifrabilitate ciclică.

<u>Teorema II.3.1</u>. Un cod H cu proprietatea de unică descifrabilitate posedă proprietatea de unică descifrabilitate infinită dacă şi numai dacă există $n_0 \in N^*$, $n_0 \leq |\mathrm{Suf}\, H \setminus H|$ astfel încît dacă $n \geq n_0$, $R_n(H) = \emptyset$.

<u>Demonstraţie</u>. Să presupunem că H posedă proprietatea de unică descifrabilitate infinită şi prin urmare şi proprietatea de unică descifrabilitate. Vom arăta că $R_n(H) = \emptyset$ pentru $n \geq n_0$, $n_0 \leq |\mathrm{Suf}\, H \setminus H|$.

Să presupunem că, în condiţiile de mai sus, $R_n(H) \neq \emptyset$ pentru $n = |\mathrm{Suf}\, H \setminus H|$. Atunci există cuvintele $p_0, p_1, \ldots p_n$ cu

$p_0 \in H$ şi $p_j \in R_j(H)$, $j = \overline{1,n}$. Cum $R_j(H) \subseteq \text{Suf } H \setminus \{e\}$ avem $p_j \in \text{Suf } H \setminus \{e\}$. Dar, $p_j \notin H$ (v.teorema II.2.5.) prin urmare $p_j \in \text{Sufp } H$, $j = \overline{1,n}$. Cum $|\text{Sufp } H| = n-1$ (deoarece $\text{Sufp } H \cup \{e\} = \text{Suf } H \setminus H$) există j_1 şi j_2 cu $1 \leq j_1 < j_2 \leq n$ astfel încît $p_{j_1} = p_{j_2}$.

Deoarece $p_{j_1} \in R_{j_1}(H)$, conform teoremei II.2.4 în care luăm $E_1 = E_2 = H$ există cuvintele $q_1, \ldots, q_{j_1+1}$ în H astfel ca să existe egalitatea ireductibilă:

(II.3.3.) $$q_1 \ldots q_{k-1} p_{j_1} = q_k \ldots q_{j_1+1} ,$$

cu $\ell(p_{j_1}) < \ell(q_{j_1+1})$ şi $q_1 \neq q_k$ (deoarece, în cazul cînd $q_1 = q_k$ egalitatea (II.3.3.) n-ar fi ireductibilă).

Intrucît $R_{j_2}(H) = (\ldots(R_{j_1}(H)\underbrace{|H)\ldots|H}_{j_2 - j_1})$ ţinînd seama de consecinţa II.2.2. are loc egalitatea:

(II.3.4.) $$p_{j_1} r_1 \ldots r_t = r'_1 \ldots r'_s p_{j_2} ,$$

cu $\ell(p_{j_1}) = \ell(p_{j_2}) < \ell(r_t)$, $r_j, r'_h \in H$, $j = \overline{1,t}$, $h = \overline{1,s}$.

In baza teoremei A.3 din egalitatea (II.3.4) urmează:

(II.3.5.) $$p_{j_1} (r_1 \ldots r_t)^n = (r'_1 \ldots r'_s)^n p_{j_1} , \quad \forall n \in N^* .$$

Din egalităţile (II.3.3.) şi (II.3.5.) obţinem succesiv:

$$q_1 \ldots q_{k-1} p_{j_1} (r_1 \ldots r_t)^n = q_1 \ldots q_{k-1} (r'_1 \ldots r'_s)^n p_{j_1} ,$$
$$, \quad \forall n \in N^* ,$$

sau

$$q_k \ldots q_{j_1+1} (r_1 \ldots r_t)^n = q_1 \ldots q_{k-1} (r'_1 \ldots r'_s)^n p_{j_1} , \quad \forall n \in N^* ,$$

ceea ce contrazice proprietatea de unică descifrabilitate infinită.

Să presupunem acum că H posedă proprietatea de unică descifrabilitate şi că $R_n(H) = \emptyset$,pentru $n \geq n_0$ cu $n_0 \leq |\text{Suf } H \setminus H|$.

Vom arăta că H posedă proprietatea de unică descifrabilitate infinită.

Să presupunem că H nu are proprietate de unică descifrabilitate infinită, deci există o egalitate de forma:

$$p_1p_2\cdots = p'_1p'_2\cdots \ , \ p_s, p'_t \in H, s,t \in N^*,$$

cu $p_1 \neq p'_1$ şi deci

$$p_1\cdots p_j \neq p'_1\cdots p'_h, \ \forall j,h \in N^*,$$

în virtutea unicei descifrabilităţi. Atunci există $j, h \in N^*$ cu $j + k = n + 1$ astfel încît să aibă loc egalitatea ireductibilă:

$$p_1\cdots p_j = p'_1\cdots p'_h w \ ,$$

cu $\ell(w) < \ell(p_j)$, ceea ce implică $w \in R_n(H)$ (v.teorema II.2.4), contrazicînd ipoteza $R_n(H) = \emptyset$, pentru $n \geq n_0$. ■

Teorema II.3.2. Codul H cu proprietatea de unică descifrabilitate posedă proprietatea de unică descifrabilitate ciclică dacă şi numai dacă există $n_0 \in N^*$, $n_0 \leq |\text{Suf } H \setminus H|$ astfel încît, dacă $n \geq n_0$, atunci $\tilde{R}_n(H) = \emptyset$, unde $\tilde{R}_n(H) = R_n(H, \text{Sufp } H)$.

Demonstraţie. Să presupunem că H posedă proprietatea de unică descifrabilitate ciclică. Dacă am avea $\tilde{R}_n(H) \neq \emptyset$ cu $n = |\text{Suf } H \setminus H|$, atunci ar exista cuvintele $p_0, p_1, \ldots, p_n$ cu $p_0 \in \text{Sufp } H$, $p_j \in \text{Suf } H \setminus \{e\}$ şi $p_j \in \tilde{R}_j(H)$, $j = \overline{1,n}$. Deoarece codul posedă proprietatea de unică descifrabilitate vom arăta, ţinînd seama de consecinţa II.2.1 că, codul H nu conţine decît cel mult un cuvînt p_j.

Să presupunem că $p_j, p_k \in H$ cu $k > j$. Întrucît $\tilde{R}_k(H) = (\ldots(\tilde{R}_j(H) \mid \underbrace{H)\ldots|H}_{k-j})$ găsim $p_k = |\ldots \| p_j \, q_1\cdots q_{k-j}$, cu $q_\ell \in H$, $\ell = \overline{1,k-j}$. De aici rezultă existenţa cuvintelor $r_1, \ldots, r_{k-j} \in H$ şi a lui $m \in N^*$, $m < k-j$, astfel încît au loc una din următoarele două egalităţi ireductibile:

1) $p_j\ r_1 \dots r_m\ p_k = r_{m+1} \dots r_{k-j}$, cu $\ell(p_k) < \ell(r_{k-j})$,

sau

2) $p_j\ r_1 \dots r_m = r_{m+1} \dots r_{k-j}\ p_k$, cu $\ell(p_k) < \ell(r_m)$,

ceea ce contrazice unica descifrabilitate. Deci n dintre cuvintele $\{p_0, \dots, p_n\}$ aparţin lui SufpH. Cum $|\text{SufpH}| = n-1$ există j_1, j_2 cu $i \leq j_1 < j_2 \leq n$ astfel ca $p_{j_1} = p_{j_2}$.

In baza consecinţei II.2.2. are loc egalitatea:

(II 3.6.) $p_{j_1}\ v_1 \dots v_t = v'_1 \dots v'_s\ p_{j_1}$,

cu $\ell(p_{j_1}) < \ell(v_t)$, $v_1, \dots, v_t, v'_1, \dots, v'_s \in H$.

Avem $p_{j_i} \neq v'_1 \dots v'_z$ cu $1 \leq z \leq s$, deoarece în caz contrar ar avea loc egalitatea:

$$v'_1 \dots v'_z\ v_1 \dots v_t = v'_1 \dots v'_z v'_{z+1} \dots v'_s v'_1 \dots v'_z,$$

cu $v_t \neq v'_z$ (deoarece $\ell(v'_z) < \ell(p_{j_1}) < \ell(v_t)$), ceea ce ar contrazice proprietatea de unică descifrabilitate.

Prin urmare $p_{j_1} = v'_1 \dots v'_z\ u$ cu $0 \leq z < s$ şi $u \neq e$, $u \in \text{Prefp}\{v'_{z+1}\}$. Inlocuind pe p_{j_1} în egalitatea (II.3.6) obţinem:

$$v'_1 \dots v'_z\ u\ v_1 \dots v_t = v'_1 \dots v'_s\ v'_1 \dots v'_z\ u,$$

sau

$$u\ v_1 \dots v_t = v'_{z+1} \dots v'_s\ v'_1 \dots v'_z\ u,$$

cu

$0 < \ell(u) < \ell(v'_{z+1})$, ceea ce contrazice proprietatea de unică descifrabilitate ciclică a codului.

Să presupunem acum că H posedă proprietatea de unică descifrabilitate şi că $R_n(H) = \emptyset$ pentru $n \geq n_0$ şi $n_0 \leq |\text{Suf } H \setminus H|$. Vom arăta că H posedă proprietatea de unică descifrabilitate ciclică.

Să presupunem contrariul. Are loc o egalitate de forma:

(II.3.7.) $u\, p_1 \cdots p_k = p'_1 \cdots p'_\ell\, u,$

cu $\ell \geq 1$, $0 < \ell(u) < \ell(p'_1)$.

Fără a restrînge generalitatea putem presupune că $\ell(u) < \ell(p_k)$. Într-adevăr, dacă $\ell(u) \geq \ell(p_k)$ atunci u s-ar putea scrie $u = u'\, p_j \cdots p_k$ [1] cu $1 < j \leq k$ și $u' \in \mathrm{Suf}_P \{p_{j-1}\}$ și ar urma:

$$u'\, p_j \cdots p_k\, p_1 \cdots p_k = p'_1 \cdots p'_\ell\, u'\, p_j \cdots p_k,$$

de unde s-ar obține, prin simplificare

(II.3.8) $u'\, p_j \cdots p_k\, p_1 \cdots p_{j-1} = p'_1 \cdots p'_\ell\, u'$,

deci o egalitate de forma (II.3.7) cu $\ell \geq 1$, $0 < \ell(u') < \ell(p'_1)$ și $\ell(u') < \ell(p_{j-1})$.

In virtutea teoremei A.3. avem, pentru orice $n \in N^*$,

(II.3.9)

$$u'(p_j \cdots p_k\, p_1 \cdots p_{j-1})^n = (p'_1 \cdots p'_\ell)^n\, u',$$

și putem presupune, fără a restrînge generalitatea, că $\ell + k \geq |\mathrm{Suf}\, H \setminus H|$, deoarece în caz contrar am putea înlocui egalitatea (II.3.8) cu egalitatea (II.3.9) alegîndu-l pe n suficient de mare.

Am ajuns astfel la o egalitate de forma (II.3.7) pentru care: $\ell \geq 1$, $0 < \ell(u) < \min\{\ell(p'_1), \ell(p_k)\}$ și $k + \ell \geq |\mathrm{Suf}\, H \setminus H|$.

Cum $\tilde{R}_n(H) = \emptyset$ pentru $n \geq n_0$, $n_0 < |\mathrm{Suf}\, H \setminus H|$ rezultă că $u \in \tilde{R}_{k+\ell}(H)$. In virtutea unicei descifrabilități $u \notin H$, deoarece în caz contrar am avea $u = p'_1 = p'_k$ ceea ce contrazice faptul că $\ell(u) < \min\{\ell(p'_1), \ell(p'_k)\}$.

Astfel $u \in \mathrm{Suf}_P H$.

Să arătăm că există k' și ℓ' astfel ca:

---

1) Remarcăm că $u' \neq e$, deoarece în caz contrar am avea $p_j \cdots p_k \in \mathrm{Pref}_P \{p'_1\}$, ceea ce contrazice proprietatea de unică descifrabilitate.

(II.3.1o)

$$u\, p_1 \cdots p_{k'} = p'_1 \cdots p'_{\ell'},$$

cu

$$p_{k'} \neq p'_{\ell'} \text{ și } 1 \leq k' \leq k, \quad 1 \leq \ell' \leq \ell .$$

Folosind teorema II.2.4, cum $u \notin \tilde{R}_n(H)$, putem afirma că nu există $w_o \in \mathrm{Suf}_p H$, $w_1, \ldots, w_n \in H$ astfel ca să avem una din următoarele două egalități ireductibile:

$$w_o w_1 \cdots w_{k-1}\, u = w_k \cdots w_n, \text{ cu } \ell(u) < \ell(w_n),$$

sau

$$w_o w_1 \cdots w_{k-1} = w_k \cdots w_n\, u, \text{ cu } \ell(u) < \ell(w_{k-1}).$$

Din egalitatea (II.3.7) putem scrie

$$t\, p_{k'+1} \cdots p_k = p'_{\ell'+1} \cdots p'_{\ell'} u,$$

$t \in \mathrm{Suf}\,\{p_{k'}\}$. Este clar că există k' astfel ca $t = e$ pentru a nu contrazice considerațiile de mai sus.

Deci

(II.3.11) $$p_{k'+1} \cdots p_k = p'_{\ell'+1} \cdots p'_{\ell}\, u, \text{ cu } p_{k'+1} \neq p'_{\ell'+1},$$

de unde din egalitatea (II.3.7) obținem egalitatea (II.3.1o).

$$u\, p_1 \cdots p_{k'} = p'_1 \cdots p'_{\ell'}$$

Din (II.3.1o) și (II.3.11) obținem egalitatea:

$$p_{k'+1} \cdots p_k\, p_1 \cdots p_{k'} = p'_{\ell'+1} \cdots p'_{\ell}\, p'_1 \cdots p'_{\ell'},$$

cu

$k' \geq 1$, $\ell' \geq 1$, $p_{k'+1} \neq p'_{\ell'+1}$, ceea ce contrazice unica descifrabilitate. ■

Teorema II.3.3. Dacă un cod H posedă proprietatea de unică descifrabilitate ciclică atunci el posedă proprietatea de unică descifrabilitate infinită.

Demonstrație. Să presupunem că H având proprietatea de unică descifrabilitate ciclică nu posedă proprietatea de unică descifrabilitate infinită. Cum H posedă proprietatea de unică

descifrabilitate (v.observaţia II.3.2) conform teoremei II.3.1, $R_n(H) \neq \emptyset$ pentru $n \leq n_o = |Suf\ H \setminus H|$ (deoarece dacă ar exista $n_1 \leq |Suf\ H \setminus H|$ şi $R_{n_1}(H) = \emptyset$ atunci $R_{n_1+k}(H) = \emptyset$, $\forall k \in N^*$ şi codul H ar poseda proprietatea de unică descifrabilitate infinită).

Există atunci cuvintele $p_0, p_1, \ldots, p_{n_o}$ cu $p_0 \in H$, $p_j \in R_j(H)$, $j = \overline{1,n_o}$. Avem $\{p_1, \ldots p_{n_o}\} \subseteq Sufp\ H$ şi $|Sufp\ H| = n_o - 1$, deci există j_1, j_2 cu $1 \leq j_1 < j_2 \leq n_o$ astfel încît $p_{j_1} = p_{j_2} \in Sufp\ H$.

Cum

$p_{j_2} = |\ldots|p_{j_1} q_1 q_2 \ldots q_{j_2-j_1}$, cu $q_s \in H$, $s = \overline{1,j_2-j_1}$ rezultă că

$$p_{j_2} \in \tilde{R}_{j_2-j_1}(H).$$

Dar

$p_{j_2} = p_{j_1}$, deci

$$p_{j_2} = |\ldots|p_{j_2} q_1 q_2 \ldots q_{j_2-j_1} = |\ldots|p_{j_1} q_1 \ldots q_{j_2-j_1} q_1 \ldots q_{j_2-j_1},$$

deci

$p_{j_2} \in \tilde{R}_{2(j_2-j_1)}(H)$. Continuînd la rel obţinem $p_{j_2} \in \tilde{R}_{n(j_2-j_1)}(H)$, $\forall n \in N^*$, deci oricare ar fi $t \in N^*$ există $s \in N^*$ astfel ca $s > t$ şi $\tilde{R}_s(H) \neq \emptyset$, ceea ce contrazice proprietatea de unică descifrabilitate ciclică (v.teorema II.3.2.). ■

Observaţia II.3.3. Fie CUD(I), CUDC(I), CUDI(I) clasele de coduri peste alfabetul finit I avînd respectiv proprietăţile de unică descifrabilitate, unică descifrabilitate ciclică şi unică descifrabilitate infinită. Atunci:

$$CUD(I) \supseteq CUDC(I) \supseteq CUDI(I)$$

§ II.4. Coduri decodabile

Teorema II.4.1. Fie E_1 un complex finit, $E_1 \subseteq I^*$ şi $E_2 \subseteq I^*$.

Atunci următoarele afirmaţii sînt echivalente:

i) $R_{n_o}(E_1,E_2) = \emptyset$ pentru un $n_o \geq 1$.

ii) Există $n \in N^*$ astfel încît dacă există o egalitate ireductibilă de forma $p\hat{m}w = \hat{m}'$ sau $p\hat{m} = \hat{m}'w$, unde $p \in E_2$, $m, m' \in E_1^*$ şi $w \in E_1$, ou $\ell(\hat{m}) + \ell(\hat{m}') \geq n$ atunci $\ell(w) \geq \ell(q)$, unde q este ultimul cuvînt din mesajul m după cum $p\hat{m}w = \hat{m}'$ sau $p\hat{m} = \hat{m}'w$. (m' sau din mesajul)

Demonstraţie. i) $\Rightarrow$ ii). Să presupunem că $R_{n_o}(E_1,E_2) = \emptyset$. Să alegem $n = n_o \ell_{max}$, unde $\ell_{max} = \max\{\ell(r) \mid r \in E_1\}$ şi fie egalitatea ireductibilă $p\hat{m}w = \hat{m}'$ (sau $p\hat{m} = \hat{m}'w$) cu $\ell(\hat{m}) + \ell(\hat{m}') \geq n$. Să presupunem că mesajele m şi m' conţin împreună s cuvinte. Atunci $\ell(\hat{m}) + \ell(\hat{m}') \leq s\,\ell_{max}$, de unde $n \leq s\,\ell_{max}$ şi prin urmare $n_o \leq s$.

Dacă $\ell(w) < \ell(q)$, unde q este cuvîntul din enunţ atunci, în baza teoremei II.2.4. avem $w \in R_s(E_1,E_2)$, ceea ce este absurd, deoarece $R_{n_o}(E_1,E_2) = \emptyset$ şi $n_o \leq s$ antrenează $R_s(E_1,E_2) = \emptyset$ (v.observaţia II.2.5). Deci $\ell(w) \geq \ell(q)$ şi are loc ii).

Să arătăm că ii) $\Rightarrow$ i). Să presupunem deci, că are loc ii) pentru $n \geq 1$. Fie $n_o \in N$ cu proprietatea $n_o > n/\ell_{min}$, unde $\ell_{min} = \min\{\ell(r) \mid r \in E_1\}$ şi $R_{n_o}(E_1,E_2) \neq \emptyset$.

Fie $w \in R_{n_o}(E_1,E_2)$. In baza teoremei II.2.4. există $p \in E_2$ şi $m,m' \in E_1^*$, cu un număr total de n_o cuvinte din E_1 astfel încît să aibă loc una din egalităţile ireductibile $p\hat{m}w = \hat{m}'$ sau $p\hat{m} = \hat{m}'w$ cu $\ell(w) < \ell(q)$.

Cum $\ell(\hat{m}) + \ell(\hat{m}') \geq n_o \ell_{min} \geq n$ obţinem o contrazicere a ipotezei ($\ell(w) \geq \ell(q)$). ■

Pentru un cod decodabil (cod cu întîrziere mărginită)H, există $n \in N^*$ astfel încît dacă m, $m_1 \in H^*$ şi $\hat{m}$ şi $\hat{m}_1$ au în comun primii n simboli, atunci $m(1) = m_1(1)$, (v.definiţia I.3.2.).

Teorema II.4.2. O mulțime finită $H \subseteq I^*$ este cod cu întîrziere mărginită dacă și numai dacă există $n' \in N^*$, astfel încît dacă $\hat{m}w = \hat{m}'$, $m, m' \in H^*$, $w \in \text{Pref } H$ și $\ell(\hat{m}') \geq n'$, atunci sau $m(1) = m'(1)$ sau $\ell(w) > \ell(q)$, unde $q = m(*)$.

Demonstrație. Fie H un cod cu întîrziere n. Să alegem $n' = n$ și să presupunem că $\hat{m}w = \hat{m}'$, unde w este un prefix al unui cuvînt din H și $\ell(\hat{m}') \geq n$. Atunci există $w' \in I^*$ astfel ca $ww' = p \in H$. Astfel $\hat{m}p = \hat{m}ww' = \hat{m}'w'$ și deci mesajele mp și m' au în comun cel puțin primii n simboli. Ca atare mesajele mp și m' au același prim cuvînt și deci și mesajele m și m' au același prim cuvînt, $m(1) = m'(1)$.

Reciproc, să presupunem că H satisface condiția din enunț. Fie $n = n' + \ell_{max}$, unde $\ell_{max} = \max \{\ell(r) \mid r \in H\}$ și $\hat{m} = p_1 p_2 \cdots$, $\hat{m}' = p'_1 p'_2 \cdots$ două mesaje avînd în comun primii n simboli, al n-lea simbol comun apărînd în cuvintele p_{t+1} și p'_{u+1} respectiv. Atunci $p_{t+1} = xx'$, $p'_{u+1} = vv'$ și $p_1 \cdots p_t\, x = p'_1 \cdots p'_u\, v$, cu $\ell(p_1 \cdots p_t\, x) = \ell(p'_1 \cdots p'_u\, v) = n$.

Să presupunem că $\ell(x) \leq \ell(v)$. Atunci $v = v''x$ și din $p_1 \cdots p_t x = p'_1 \cdots p'_u v''x$ obținem $p_1 \cdots p_t = p'_1 \cdots p'_u v''$. Dacă $\ell(v'') > \ell(p_t)$ simplificînd cu p_t găsim: $p_1 \cdots p_{t-1} = p'_1 \cdots p'_u v'''$, unde $v'' = v'''p_t$. Dacă $\ell(v''') > \ell(p_{t-1})$ simplificăm cu p_{t-1} ș.a.m.d. In sfîrșit, ajungem la o egalitate de forma:

(II.4.1) $\qquad p_1 \cdots p_r = p'_1 \cdots p'_u z$,

cu $\ell(z) \leq \ell(p_r)$ și z este un prefix al lui p'_{u+1}. Avem $\ell(p'_1 \cdots p'_u z) \geq \ell(p'_1 \cdots p'_u v) - \ell_{max} = n - \ell_{max} = n'$, deci egalitatea (II.4.1) satisface condițiile din enunț. Cum $\ell(z) \leq \ell(p_r)$ obținem $p_1 = p'_1$. ■

Teorema II.4.3. Fie H un c.u.d.finit. Următoarele condiții sînt echivalente:

i)Există $n_o \in N^*$ astfel încît: $R_{n_o}(H) = \emptyset$.

ii)Există $n \in N^*$ astfel încît dacă în egalitatea ireductibilă $\hat{m}w = \hat{m}'$, $m,m' \in H^*$, avem $\ell(\hat{m}) + \ell(\hat{m}') \geq n$ atunci $\ell(w) \geq \ell(q)$, unde $q = m'(*)$.

iii)Există $n' \in N^*$ astfel ca în egalitatea $\hat{m}z = \hat{m}'$, cu $z \in$ Pref H şi $\ell(\hat{m}') \geq n'$ să avem sau $m(1) = m'(1)$ sau $\ell(z) > \ell(q)$.

iv) H este un cod cu întîrziere mărginită.

Demonstraţie. Echivalenţa afirmaţiilor i) şi ii) este conţinută în teorema II.4.1. luînd $E_1=E_2=H$. In acest caz p din enunţul teoremei II.4.1. aparţine lui H şi $pm \in H^*$.

Echivalenţa afirmaţiilor iii) şi iv) a fost demonstrată prin teorema II.4.2.

Rămîne să arătăm echivalenţa dintre ii) şi iii).

ii)$\Rightarrow$iii).Să alegem $n'=n$ şi să presupunem că $\hat{m}z = \hat{m}'$ cu z un prefix al unui cuvînt din H şi $\ell(\hat{m}') \geq n'$.
Atunci $\ell(\hat{m}) + \ell(\hat{m}') \geq n' = n$ şi deci $\ell(\hat{m}) + \ell(\hat{m}') \geq n$.
Dacă egalitatea $\hat{m}z = \hat{m}'$ este ireductibilă, în baza lui ii) $\ell(z) \geq \ell(q)$. Mai mult $\ell(z) \neq \ell(q)$ deoarece, în caz contrar egalitatea $\hat{m}z = \hat{m}'$ n- ar fi ireductibilă. Rămîne deci $\ell(z) > \ell(q)$.

Dacă egalitatea $\hat{m}z = \hat{m}'$ nu este ireductibilă atunci $\hat{m} = \hat{m}_1\hat{m}_2z$ şi $\hat{m}' = \hat{m}'_1\hat{m}'_2$ cu $\hat{m}_1=\hat{m}'_1$ şi $\hat{m}_2z = \hat{m}'_2$. Din proprietatea de unică descifrabilitate a lui H şi din $\hat{m}_1=\hat{m}'_1$ urmează că m_1 şi m'_1 şi prin urmare şi m şi m' au acelaşi prim cuvînt.

iii)$\Rightarrow$ii). Să alegem $n = 2(n'+\ell_{max})$ cu $\ell_{max} = \max\{\ell(p) \mid p \in H\}$ şi fie egalitatea ireductibilă $\hat{m}w = \hat{m}'$ cu $\ell(\hat{m}) + \ell(\hat{m}') \geq n$. Să presupunem că afirmaţia ii) nu-i adevărată, adică $\ell(w) < \ell(q)$.

Fie $\hat{m} = p_1 \ldots p_r$, $\hat{m}' = q_1 \ldots q_s q$. Atunci $p_1 \ldots p_r w = q_1 \ldots q_s q$, de unde $q = zw$. De aici $p_1 \ldots p_t = q_1 \ldots q_s z$. Dacă

$\ell(z) > \ell(p_r)$ atunci $z = z'p_r$ şi obţinem $p_1 \cdots p_{r-1} = q_1 \cdots q_s z'$. Dacă $\ell(z') > \ell(p_{r-1})$ atunci $z' = z'' p_{r-1}$ şi $p_1 \cdots p_{r-2} = q_1 \cdots q_s z''$ etc. In cele din urmă obţinem egalitatea:

(II.4.2) $$p_1 \cdots p_t = q_1 \cdots q_s y,$$

în care $\ell(y) \leq \ell(p_t)$ şi y este un prefix al lui q.

Avem $\ell(\hat{m}) = \ell(\hat{m}') - \ell(w)$, deci $2\ell(\hat{m}') - \ell(w) = \ell(\hat{m}) + \ell(\hat{m}') \geq n$ şi astfel $\ell(\hat{m}') \geq n/2 = n' + \ell_{max}$. Deoarece y este un prefix al lui q avem $\ell(q_1 \cdots q_s y) \geq \ell(q_1 \cdots q_s q) - \ell_{max} = \ell(\hat{m}') - \ell_{max} \geq n'$. Aplicînd propoziţia iii) egalităţii (II.4.2) în care $\ell(y) \leq \ell(p_z)$ urmează că mesajele $(p_1, \ldots, p_t)$ şi $(q_1, \ldots q_s)$ au $p_1 = q_1$, ceea ce contrazice ireductibilitatea egalităţii $\hat{m}w = \hat{m}'$. ■

Vom da în continuare o proprietate numerică a mulţimilor reziduale care permite obţinerea unui algoritm de verificare a proprietăţii de întîrziere mărginită a unui cod.

<u>Teorema II.4.4</u> Fie H un cod pe I, $E \subseteq I^*$ şi fie t numărul sufixelor cuvintelor din $H \cup E$, sufixe care nu aparţin lui H. Dacă există $n \in N^*$ astfel ca $R_n(H,E) = \emptyset$ atunci $R_{t+2}(H,E) = \emptyset$.

Dacă cuvintele din E sînt sufixe ale cuvintelor din codul H atunci $R_{t+1}(H,E) = \emptyset$.

<u>Demonstraţie</u>. Să presupunem că $R_{t+2}(H,E) \neq \emptyset$ şi $p_{t+2} \in R_{t+2}(H,E)$. Atunci $R_j(H,E) \neq \emptyset$, $j = \overline{1,t+2}$ şi există un şir de cuvinte $p_0, p_1, \ldots p_{t+2}$ cu $p_j \in R_j(H,E)$ şi $p_{j+1} = p_j | q_j$, unde $q_j \in H$. Să observăm că $p_j \neq p_k$ pentru $j \neq k$, deoarece, dacă $p_j = p_k$ cu $j \neq k, j < k$ atunci $p_j \in R_{k+(k-j)}(H,E)$, $p_j \in R_{k+2(k-j)}(H,E), \ldots$ şi, în general $p_j \in R_{k+m(k-j)}(H,E), \forall m \in N^*$. Intr-adevăr $p_k = \| \ldots | p_j q_1 \cdots q_{k-j} = \| \ldots | p_k q_1 \cdots q_{k-j}$, deci $p_k \in R_{k+(k-j)}(H,E)$ etc. Prin urmare, $R_n(H,E) \neq \emptyset, \forall n \in N^*$ (deoarece, în caz contrar, dacă $R_m(H,E) = \emptyset$ atunci $R_{m+k}(H,E) = \emptyset, \forall k \in N$), ceea ce contrazice

ipoteza.

Remarcăm că şirul de cuvinte $p_0, p_1, \ldots p_{t+2}$ conţine cel mult un cuvînt din H, deoarece, dacă $p_j, p_k \in H$ cu $j \neq k$ atunci $p_k \in R_{k-j}(H,H) = R_{k-j}(H)$, ceea ce contrazice unica descifrabilitate (v.teorema II.2.5).

Astfel, orice cuvînt din mulţimea $\{p_0, p_1, \ldots, p_{t+2}\}$, cu excepţia posibilă a lui $p_0 \in E$, este sufix al cuvintelor din $H \cup E$. Aceasta conduce la contrazicerea ipotezei care afirma existenţa a t astfel de sufixe.

Deci $R_{t+2}(H,E) = \emptyset$.

Dacă cuvintele din E sînt sufixe ale cuvintelor din H atunci şi p_0 este un astfel de sufix şi deci $R_{t+1}(H,E) = \emptyset$. ■

Teorema II.4.5. Codul H este cu întîrziere mărginită dacă şi numai dacă $R_{t+1}(H) = \emptyset$ unde $t = |\mathrm{Sufp}\ H|$.

Demonstraţie. Propoziţia se obţine imediat din teorema II.4.3. i) şi teorema precedentă. ■

Observaţia II.4.1. Din teorema II.3.1. rezultă că un c.u.d. este decodabil dacă şi numai dacă posedă proprietatea de unică descifrabilitate infinită.

Exemplul II.4.1. Fie $I = \{0,1\}$ şi $H = \{01, 0110100\}$. Atunci

$R_0(H)$	$R_1(H)$	$R_2(H)$
01	10100	
0110100		

Deoarece $R_2(H) = \emptyset$, codul H este decodabil.

Exemplul II.4.2. Fie $I = \{0,1\}$ şi $H = \{0001, 00101, 11001, 01101, 0011011, 1111011, 0010111\}$.

Avem:

$R_0(H)$	$R_1(H)$	$R_2(H)$
00001	11	001
00101		11011
11001		
01101		
0011011		
1111011		
0010111		

Deoarece $R_2(H) \neq \emptyset$, codul H nu este decodabil.

§. II.5. Coduri sincronizabile

Un c.u.d.H este sincronizabil (v.definiţia I.3.3.)dacă există $n \in N^*$, astfel încît din $ur, rv \in \hat{H}^*, u,r,v \in I^*$ şi $\ell(r) \geq n$ să urmeze $r \in \hat{H}^*$.

Teorema II.5.1. Fie H un c.d.u finit. Următoarele afirmaţii sînt echivalente:

i)Există $n_0 \in N^*$ astfel încît $\tilde{R}_{n_0}(H) = \emptyset$

ii)Există $n_1 \in N^*$ astfel încît în orice egalitate ireductibilă de.forma $dm\hat{w} = \hat{m}'$ sau de forma $d\hat{m} = \hat{m}'w$, cu $d \in Suf\ H$, $m,m' \in H^*$, $w \in I^*$ şi $\ell(\hat{m}) + \ell(\hat{m}') \geq n_1$, avem $\ell(w) \geq \ell(q)$, unde q este ultimul cuvînt din m' sau m respectiv.

iii)Există $n_2 \in N^*$, astfel încît din $ur, rv \in \hat{H}^*$, $u,r,v \in I^*$ şi $\ell(r) \geq n_2$ să urmeze $r \in \hat{H}^*$, adică codul H este sincronizabil.

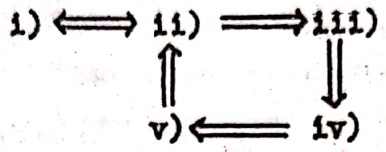
iv)Există $n_3 \in N^*$, astfel încît:

1)dacă $r \in I^*$, $\ell(r) \geq n_3$ şi există $u \in I^*$ cu $ur \in \hat{H}^*$, atunci $v_1 r\ v_2 \in \hat{H}^*$ implică $v_1 r \in \hat{H}^*$.

2)dacă $r \in I^*$, $\ell(r) \geq n_3$ şi există $v \in I^*$ cu $rv \in \hat{H}^*$, atunci $u_1 r u_2 \in \hat{H}^*$ implică $r u_2 \in \hat{H}^*$.

v)Există $n_4 \in N^*$ astfel încît dacă există $u,r,v \in I^*$ cu $urv \in \hat{H}^*$ şi $\ell(r) \geq n_4$, atunci r se poate scrie sub forma $r = r_1 r_2$ şi $u'rv' \in \hat{H}^*$ implică $a'r_1 \in \hat{H}^*$ şi $r_2 b' \in \hat{H}^*$.

Demonstraţie, Vom arăta următoarele implicaţii



Echivalenţa i) ⟺ ii) rezultă din teorema II.4.1 cu $E_1 = H$ şi $E_2 = \text{Suf } H$.

ii) ⟹ iii) Alegem $n_2 = n_1$ şi fie $u,v \in I^*$ astfel încît $ur = \hat{m} \in \hat{H}^*$, $rv = \hat{m}' \in \hat{H}^*$ şi $r \in I^*$ cu $\ell(r) \geq n_2$. Vom arăta că $r \in \hat{H}^*$. Deoarece $ur \in \hat{H}^*$, ur este un produs de cuvinte din H şi simplificînd la stînga egalitatea $ur = \hat{m}$, obţinem $r = r'\hat{m}_1$ în care r' este un sufix al unui cuvînt din H. Dacă sufixul r' ar fi chiar un cuvînt din codul H, atunci $r = r'\hat{m}_1 \in \hat{H}^*$. Să presupunem deci că $r' \in \text{Sufp } H$.

Procedînd analog cu egalitatea $rv = \hat{m}'$, obţinem $v = v'\hat{m}_2$, $\hat{m}' = \hat{m}_3\hat{m}_2$ şi $\ell(v') < \ell(q)$, unde q este ultimul cuvînt din m_3. Dacă $\ell(v') = \ell(q)$, atunci v' ar fi ultimul cuvînt din m_3 şi $v \in \hat{H}^*$, deci $r \in \hat{H}^*$. Avem, deci $rv' = \hat{m}_3$ sau $r'\hat{m}_1 v' = \hat{m}_3$. In această ultimă egalitate $r' \in \text{Sufp } H$ şi $\ell(v') < \ell(q)$.

Din $\hat{m}_3 = rv'$, urmează $\ell(\hat{m}_3) \geq \ell(r)$ şi deci cu atît mai mult, $\ell(\hat{m}_1) + \ell(\hat{m}_3) \geq \ell(r) \geq n_2 = n_1$. Dacă egalitatea $r'\hat{m}_1 v' = \hat{m}_3$ ar fi ireductibilă, atunci în baza lui ii) ar urma $\ell(v') \geq \ell(q)$, deci o contradicere. Prin urmare egalitatea $r'\hat{m}_1 v' = \hat{m}_3$ nu este ireductibilă şi simplificînd-o obţinem $r'\hat{m}_4 = \hat{m}_5$, cu $m_4, m_5 \in H^*$. Atunci $r'\hat{m}_4 \in \hat{H}^*$ şi deci şi $r'\hat{m}_1 = r \in \hat{H}^*$.

iii) $\Rightarrow$ iv$_1$). Să alegem $n_3 = n_2 + \ell_{max}$, unde $\ell_{max} = \max\{\ell(p) \mid p \in H\}$ și să presupunem că există $u \in I^*$, astfel încît $ur \in \hat{H}^*$, cu $\ell(r) \geq n_3$. Fie $v_1 r v_2 \in \hat{H}^*$. Vom arăta că $v_1 r \in \hat{H}^*$. Fie y cuvîntul format din primii ℓ_{max} simboli din r. Din $v_1 r v_2 \in \hat{H}^*$, urmează că $v_1 r v_2$ este un produs de cuvinte din H, și deoarece fiecare cuvînt din H are lungimea cel mult egală cu ℓ_{max}, în cuvîntul y există un simbol care este primul simbol al unui cuvînt din H, ce apare în $v_1 r v_2$. Așa dar r se poate scrie sub forma $r = r_1 r_2$ cu $v_1 r_1$, $r_2 v_2 \in \hat{H}^*$, cuvîntul r_2 este un prefix pentru $r_2 v_2 \in \hat{H}^*$ și un sufix pentru $ur_1 r_2 = ur \in \hat{H}^*$. Cum $\ell(r_2) \geq \ell(r) - \ell_{max} \geq n_3 - \ell_{max} = n_2$, putem aplica iii) și rezultă că $r_2 \in \hat{H}^*$, dar atunci și $v_1 r_1 r_2 = v_1 r \in \hat{H}^*$.

iii $\Rightarrow$ iv$_2$). Se procedează similar cu cazul precedent, alegînd însă drept y cuvîntul format din ultimii ℓ_{max} simboli din r.

iv $\Rightarrow$ v). Să alegem $n_4 = 2n_3 + \ell_{max}$ și fie $urv \in \hat{H}^*$, cu $\ell(r) \geq n_4$. Fie y cuvîntul format din ℓ_{max} simboli din mijlocul cuvîntului r. Atunci în urv există un cuvînt din H al cărui prim simbol se găsește printre simbolii cuvîntului y. Corespunzător r se poate scrie sub forma $r = r_1 r_2$, cu ur_1, $r_2 v \in \hat{H}^*$. Cum $\min\{\ell(r_1), \ell(r_2)\} \geq \frac{\ell(r) - \ell_{max}}{2} \geq \frac{n_4 - \ell_{max}}{2} = n_3$, putem aplica iv) și din $u'rv' = u'r_1 r_2 v' \in \hat{H}^*$, urmează $u'r_1$, $r_2 v' \in \hat{H}^*$.

v $\Rightarrow$ ii). Să alegem $n_1 \geq 2(n_4 + 2\ell_{max})$ și fie egalitatea ir ductibilă $dm = \hat{m}$ cu $d \in Suf\ H$ și $\ell(\hat{m}) + \ell(\hat{m}') \geq n_1$.

Dacă $\ell(w) < \ell(q)$, unde q este ultimul cuvînt din $\hat{m}$, atunci, deoarece $\ell(\hat{m}) = \ell(\hat{m}') - \ell(d) - \ell(w)$, avem $\ell(\hat{m}) + \ell(\hat{m}') = 2\ell(\hat{m}') - \ell(d) - \ell(w)$ și deci $2\ell(\hat{m}') - \ell(d) - \ell(w) \geq n_1$. Prin urmare $\ell(\hat{m}') \geq n_1/2$ și $\ell(\hat{m}) \geq n_1/2 - \ell(d) - \ell(w) \geq n_1/2 - 2\ell_{max} \geq n_4$.

Deci $d\hat{m}w \in \hat{H}^*$ cu $\ell(\hat{m}) \geq n_4$; atunci în baza lui v), mesajul m se poate scrie sub forma $m = m_1 m_2$ cu $d\hat{m}_1, \hat{m}_2 w \in \hat{H}^*$. Aplicînd proprietatea de unică descifrabilitate a lui H, egalităţii $d\hat{m}_1\hat{m}_2 w = \hat{m}'$, rezultă că $\hat{m}'$ este format din subcuvintele $d\hat{m}_1$, $\hat{m}_2 w \in \hat{H}^*$, şi deci egalitatea $d\hat{m}w = \hat{m}'$, nu este ireductibilă, ceea ce contrazice presupunerea făcută. Urmează că ipoteza $\ell(w) < \ell(q)$ este falsă şi rămîne $\ell(w) \geq \ell(q)$.

Fie acum egalitatea ireductibilă $d\hat{m} = \hat{m}'w$, cu $d \in \text{suf } H$ şi $\ell(\hat{m}) + \ell(\hat{m}') \geq n_1$. Deoarece $d \in \text{Suf } H$, există $p \in I^*$, astfel ca $pd \in H$ şi $pd\hat{m} = p\hat{m}'w \in \hat{H}^*$. Dar $\ell(\hat{m}') = \ell(\hat{m}) + \ell(d) - \ell(w)$ şi $\ell(\hat{m}) + \ell(\hat{m}') = 2\ell(\hat{m}) + \ell(d) - \ell(w)$, deci $2\ell(\hat{m}) + \ell(d) - \ell(w) \geq n_1$, sau $\ell(\hat{m}) \geq \frac{n_1 + \ell(w) - \ell(d)}{2}$.

Astfel $\ell(\hat{m}') = \ell(\hat{m}) + \ell(d) - \ell(w) \geq \frac{n_1 + \ell(w) - \ell(d)}{2} + \ell(d) - \ell(w)$, de unde are loc inegalitatea:

(II.5.1) $\ell(\hat{m}') \geq \frac{n_1}{2} - \frac{\ell(w)}{2} + \frac{\ell(d)}{2} \geq \frac{n_1}{2} - \frac{\ell(w)}{2}$.

Dacă $\ell(w) < \ell(q)$, unde q este ultimul cuvînt din m atunci inegalitatea (II.5.1) devine $\ell(\hat{m}') \geq \frac{n_1}{2} - \frac{\ell_{max}}{2} \geq \frac{n_1}{2} - \ell_{\geq n_4}$. Aplicînd v) lui m', ca un sub cuvînt al lui $p\hat{m}w \in \hat{H}^*$, urmează $\hat{m}' = \hat{m}'_1\hat{m}'_2$, cu $p\hat{m}'_1$, $\hat{m}'_2 w \in \hat{H}^*$. Avem deci $pd\hat{m} = p\hat{m}'_1\hat{m}'_2 w$. In baza proprietăţii de unică descifrabilitate a lui H, urmează că $p\hat{m}'_1$ şi $\hat{m}'_2 w$ sînt subcuvinte din $pd\hat{m}$. Deoarece pd este primul cuvînt din $pd\hat{m}$ şi deci şi din $p\hat{m}'_1$, mesajul $m \in H^*$ trebuie să se descompună sub forma $m = m_1 m_2$, astfel încît $pd\hat{m}_1 = p\hat{m}'_1$ şi $\hat{m}_2 = \hat{m}'_2 w$, dar aceasta contrazice ireductibilitatea egalităţii $d\hat{m} = \hat{m}'w$. Prin urmare presupunerea $\ell(w) < \ell(q)$ este falsă şi avem $\ell(w) \geq \ell(q)$. ■

Observaţia II.5.1. Condiţia i) din teorema precedentă oferă un algoritm de verificare dacă un c.u.d.finit este sincronizabil.

Mai mult în baza teoremei II.3.2. un cod este sincronizabil dacă şi numai dacă este corector şi posedă proprietatea de unică descifrabilitate ciclică.

Teorema II.5.2. C.u.d. finit H este sincronizabil dacă şi şi numai dacă $\tilde{R}_{t+1}(H) = \emptyset$, unde $t = |Sufp\ H|$.

Demonstraţie. Rezultatul se obţine din teoremele II.5.1. i), II.4.4. luînd E = Sufp H şi ţinînd seama de definiţia lui Sufp H. ■

Exemplul II.5.1. Fie $I = \{0,1\}$ şi $H = \{1,10,011,0010\}$, codul considerat în exemplul II.2.7., despre care am arătat că posedă proprietatea de unică descifrabilitate.

Atunci $Suf\ H \setminus (H \cup \{e\}) = \{0,11,010\}$, deci $|Sufp\ H| = 3$.

Avem:

$\tilde{R}_0(H)$	$\tilde{R}_1(H)$	$\tilde{R}_2(H)$	$\tilde{R}_3(H)$	$\tilde{R}_4(H)$
0	1	0	0	1
11	11	1	11	11
010	010		010	010

Codul H nu este sincronizabil, deoarece $\tilde{R}_4(H) \neq \emptyset$.

Exemplul II.5.2 Fie $I = \{0,1\}$ şi $H = \{0001011, 00111001\}$.

Codul H este sincronizabil, aşa cum se poate constata imediat.

In tabelul următor scoatem în evidenţă caracterizări explicite ale codurilor de diverse tipuri, comparînd între ele afirmaţii "asemănătoare".

Proprietatea codului H	Afirmaţie echivalentă
Cod unic descifrabil	$R_n(H) \cap H = \emptyset, \forall n \in H^*$
Cod cu unică descifrabilitate ciclică	$R_n(H, Sufp\ H) \neq \emptyset$, $n \geq n_o$ şi $n_o \leq \lvert Suf\ H \setminus H \rvert$
Cod cu unică descifrabilitate infinită	$R_n(H) = \emptyset$, $n \geq n_o$ şi $n_o \leq \lvert Suf\ H \setminus H \rvert$.
Cod decodabil	$\exists n \in N^*$ cu $R_n(H) = \emptyset$
Cod sincronizabil	$R_n(H) \cap H = \emptyset$, $\forall n \in N^*$ şi $\exists\, n \in N^*$ cu $R_n(H, SufpH) = \emptyset$

Scanned with OKEN Scanner

Partea III-a

Coduri cu lungime variabilă pentru canale cu zgomot

Scanned with OKEN Scanner

§ III.1 Noţiunea de mulţime calibrată

Mulţimile calibrate introduse de W.E.Hartnett [30] constituie o extindere a noţiunii de cod. Utilizarea lor a permis obţinerea unor caracterizări ale unor clase de coduri cu lungime variabilă pentru canale cu zgomot, analoage caracterizărilor date de Sardinas-Patterson, Levenştein şi Riley pentru aceste clase de coduri, pentru canale fără zgomot.

Fie un alfabet finit cu $|I| \geq 2$ şi I^* semigrupul liber generat de I.

Pentru orice cuvînt $r \in I^*$, introducem mulţimea

$$[r] = \{r' \mid r' \in I^*,\ \ell(r') = \ell(r)\}.$$

Astfel, mulţimea $[r]$ conţine toate cuvintele din I^*, de lungime egală cu lungimea lui r. Avem $|[r]| < \infty$, $\forall r \in I^*$.

Fie $H \subset I^*$. Vom nota cu $[H] = \bigcup \{[p] \mid p \in H\}$.

Definiţia III.1.1. O aplicaţie de calibrare pentru o mulţime finită $H \subset I^*$ este o aplicaţie $\beta : H \to P([H])$, care se bucură de următoarea proprietate:

$$\beta(p) \subset [p],\ \forall p \in H.$$

Definiţia III.1.28 O mulţime calibrată pe alfabetul I, este o pereche (H, β) cu $H \subset I^*$ şi $|H| < \infty$, iar β o aplicaţie de calibrare pentru H.

Exemplul III.1.1. Fie $I = \{0,1\}$ şi $H = \{001, 1010, 01010\}$. Aplicaţie de calibrare $\beta : H \to P([H])$ este definită prin următorul tablou:

$\beta(001)$	$\beta(1010)$	$\beta(01010)$
001	1010	01010
010	1100	11000
100	1001	10100
	0110	10010
	0101	10001
	0011	01100
		01001
		00110
		00101
		00011

In acest caz numărul de simboli egali cu 1 în orice $v \in \beta(p)$, $\forall p \in H$, coincide cu numărul de simboli egali cu 1 din p.

Observaţia III.1.1. O aplicaţie de admisibilitate (v.definiţia I.1.1.) este o aplicaţie de calibrare, iar un cod (v.definiţia I.1.2.) este o mulţime calibrată.

Ca şi în cazul codurilor, alegerea aplicaţiei de calibrare reflectă unele proprietăţi ale canalului de transmisie.

In general pentru o aplicaţie de calibrare nu avem $p \in \beta(p)$.

Dacă însă mulţimea $\beta(p)$ este interpretată ca fiind formată din acele cuvinte din I^*, de lungime egală cu lungimea lui p, şi care atunci cînd sînt recepţionate sînt decodificate în p, aplicaţia de calibrare trebuie să fie o aplicaţie de admisibilitate.

De aceea în aplicaţii practice se consideră acele aplicaţii de calibrare care sînt şi aplicaţii de admisibilitate, deci acele mulţimi calibrate (H, β) care sînt coduri.

Observaţia III.1.2. Aplicaţia $\iota : H \to P([H])$ dată prin $\iota(p) = \{p\}$ este o aplicaţie de calibrare.

Perechea (H, ι) este o mulţime calibrată simplă; ori de cîte ori va fi convenabil vom interpreta (H, ι) ca fiind H.

Aplicaţia ι este chiar o aplicaţie de adminibilitate iar (H, ι) este şi cod simplu.

Fie (H, β) o mulţime calibrată. Vom nota prin

$$\beta(H) = \bigcup\{\beta(p) \mid p \in H\}.$$

Definiţia III.1.3. Multimea calibrată extinsă a mulţimii calibrate (H, β) este mulţimea calibrată $(\beta(H), \iota)$ unde ι este aplicaţia de calibrare din observaţia III.1.2.

Observaţia III.1.4. O mulţime calibrată extinsă, fiind o mulţime calibrată simplă, este un cod simplu.

Dacă (H, β) este un cod, atunci mulţimea calibrată extinsă coincide cu codul extins al codului (H, β). (v. definiţia I.1.4.).

Am observat deja că în anumite cazuri particulare mulţimile calibrate sînt coduri, (atît cu lungime variabilă cît şi coduri bloc) şi anume atunci cînd aplicaţia de calibrare este o aplicaţie de admisibilitate.

Vom arăta cum, alegînd convenabil aplicaţia de calibrare, se pot obţine şi alte clase de coduri. Pentru aceasta sînt necesare în prealabil unele rezultate care vor fi expuse în cele ce urmează:

Fie o aplicaţie $g : I \cdot I \to N$ cu proprietăţile:

i) $g(i_1, i_2) \geq 0$ şi $g(i_1, i_2) = 0 \Longleftrightarrow i_1 = i_2$,

ii) $g(i_1, i_2) = g(i_2, i_1)$, $\forall (i_1, i_2) \in I \times I$,

iii) $g(i_1, i_2) \leq g(i_1, i) + g(i, i_2)$, $i_1, i_2, i \in I$.

Aplicaţia g poate fi extinsă la $I^* \times I^*$ în felul

următor. Fie $p, q \in I^*$, $p = i_1 \ldots i_n$, $q = i'_1 \ldots i'_m$ și fie $k = \min(n,m)$. Atunci definim aplicația $\rho_g : I^* \times I^* \to N$, punînd

(III.1.1.) $$g(p,q) = \sum_{j=1}^{k} g(i_j, i'_j).$$

Observația III.1.5. Restricția aplicației ρ_g la $I \times I$ este aplicația g.

Teorema III.1.1. Aplicația $\rho_g : I^* \times I^* \to N$, dată prin formula (III.1.1.) se bucură de proprietățile:

1) $\rho_g(p,q) \geq 0$ și $\rho_g(p,q) = 0$ dacă și numai dacă $p \in \text{Pref}\{q\}$ sau $q \in \text{Pref}\{p\}$,

2) $\rho_g(p,q) = \rho_g(q,p)$, $\forall (p,q) \in I^* \times I^*$,

3) $\rho_g(p,q) \leq \rho_g(p,r) + \rho_g(r,q)$ dacă $\ell(r) \geq \min\{\ell(p), \ell(q)\}$.

Demonstrație. Este clar că $\rho_g(p,q) \geq 0$. Avem $\rho_g(p,q) = 0$, atunci și numai atunci cînd $g(i_j, i_j) = 0$, $j = \overline{1,k}$, și prin urmare ținînd seama de proprietatea i) a aplicației g, avem $i_j = i'_j$, $j = \overline{1,k}$. Atunci $p \in \text{Pref}\{q\}$ sau $q \in \text{Pref}\{p\}$, după cum $\ell(p) \leq \ell(q)$ sau $\ell(p) \geq \ell(q)$. Deci are loc 1).

Proprietatea 2) rezultă imediat din proprietatea ii) a aplicației g.

In sfîrșit fie $r \in I^*$ cu $\ell(r) \geq \min\{\ell(p), \ell(q)\}$. Să presupunem că $p = i_1 \ldots i_n$, $q = i'_1 \ldots i'_m$ și $r = i''_1 \ldots i''_h$ cu $h \geq n,m$ și fie $k = \min\{n,m\}$.

Atunci în baza proprietății iii) a aplicației g, avem $g(i_j, i'_j) \leq g(i_j, i''_j) + g(i''_j, i'_j)$, $j = \overline{1,k}$, de unde prin adunare obținem:

$$\rho_g(p,q) \leq \sum_{j=1}^{k} g(i_j, i''_j) + \sum_{j=1}^{k} g(i''_j, i'_j).$$

Dacă $k = n$, atunci $\sum_{j=1}^{k} g(i_j, i''_j) = \rho_g(p,r)$, iar

$$\rho_g(q,r) = \sum_{j=1}^{k} g(i''_j, i'_j) + \sum_{j=k+1}^{m} g(i''_j, i'_j) \geq \sum_{j=1}^{k} g(i''_j, i'_j),$$

de unde

$$\rho_g(p,q) \leq \rho_g(p,r) + \rho_g(q,r). \blacksquare$$

Definiţia III.1.4. O indexare pe mulţimea finită $H \subset I^* \setminus \{e\}$ este o aplicaţie $\theta : H \to N$.

Perechea (H, θ) se numeşte o mulţime indexată.

Fie (H, θ) o mulţime indexată. Să notăm prin

$$S_{\theta(p)}(p; \rho_g) = \{p' \mid p' \in [p], \rho_g(p,p') \leq \theta(p)\}.$$

Mulţimea $S_{\theta(p)}(p; \rho_g) \subset [p]$ se numeşte ρ_g - sferă cu centrul în p şi de rază $\theta(p)$.

Observaţia III.1.6. Aplicaţia $\beta_\theta^g : H \to P([H])$, dată prin $\beta_\theta^g(p) = S_{\theta(p)}(p; \rho_g)$, $\forall p \in H$, este o aplicaţie de calibrare. Mai mult $p \in \beta_\theta^g(p)$.

Prin urmare perechea (H, β_θ^g) este o mulţime calibrată.

Deoarece, în general $\beta_\theta^g(p) \cap \beta_\theta^g(q) \neq \emptyset$ cu $p \neq q$, perechea (H, β_θ^g) nu-i cod.

In unele cazuri, ca de exemplu atunci cînd $\ell(p) \neq \ell(q)$ $\forall p,q \in H$, aplicaţia β_θ^g este o aplicaţie de admisibilitate. Are sens de aceea:

Definiţia III.1.5. Un cod indexat este un cod (H, β_θ^g) unde aplicaţia de indexare $\theta : H \to N$ este astfel încît β_θ^g să fie o aplicaţie de admisibilitate.

Observaţia III.1.7. Se poate întîmpla că $S_{\theta(a)}(p; \rho_g) = \{a\}$, chiar pentru aplicaţii de indexare θ care iau valori mari, obţinîndu-se în acest caz, numai coduri simple, pentru canale fără zgomot.

Ca să se evite acest lucru, trebuiesc impuse condiţii asupra aplicaţiei g.

Vom prezenta în continuare unele aplicaţii g, care asigură că $S_{\theta(a)}(p; \rho_g) \neq \{a\}$.

Definiţia III.1.6. O quasi-metrică pe I, este o aplicaţie $g : I \times I \to N$ care satisface condiţiile i),ii) şi iii) şi în plus are loc

(III.1.2.) dacă $g(i_1,i_2) = h + k > 1$, $h,k \in N^*$, atunci există $i \in I$, astfel încît $g(i_1,i) = h$ şi $g(i,i_2) = k$.

Observaţia III.1.8. Condiţia (III.1.2.) din definiţia precedentă este echivalentă cu condiţia:

(III.1.3.) dacă $q \in [p]$ şi $\rho_g(p,q) = h+k > 1$, cu $h,k \in N^*$, atunci există $r \in [p]$ astfel încît $\rho_g(p,r) = h$ şi $\rho_g(r,q) = k$.

Intr-adevăr, se observă imediat că (III.1.3.) $\Longrightarrow$ $\Rightarrow$(III.1.2.),luînd $p = i_1$.

Să arătăm că (III.1.2.)$\Rightarrow$ (III.1.3.). Fie deci $p = i_1 \ldots i_n$, $q = i'_1 \ldots i'_n \in [p]$, şi $\rho_g(p,q) = h+k > 1$, $h,k \in N^*$. Avem $\rho_g(p,q) = \sum_{j=1}^{n} g(i_j,i'_j) = h+k > 1$. Să notăm cu $J = \{j \mid g(i_j,i'_j) \geq 2\}$, $J' = \{j \mid g(i_j,i'_j) = 1\}$ şi $J^\circ = \{j \mid g(i_j,i'_j) = 0\}$.

Avem evident $\{1,\ldots,n\} = J \cup J' \cup J^\circ$, $J \cup J' \neq \emptyset$, iar mulţimile J, J' şi J'' sînt disjuncte două cîte două.

Dacă $j \in J$, atunci $g(i_j,i'_j) = h_j+k_j \geq 2$ cu $h_j,k_j \in N^*$ şi $\sum_{j \in J} h_j + k_j + |J'| = h + k$. Să alegem numerele naturale h_j şi k_j astfel încît $\sum_{j \in J} h_j + h_o = h$ iar $\sum_{j \in J} k_j + |J'| - h_o = k$ cu $0 \leq h_o \leq |J'|$.

Fie $j \in J$, avem $g(i_j,i'_j) = h_j + k_j \geq 2$, $h_j,k_j \in N^*$ şi în baza lui (III.1.2.)există $i''_j \in I$ astfel încît $g(i_j,i''_j) = h_j$ $g(i'_j,i''_j) = k_j$ şi deci $g(i_j,i'_j) = g(i_j,i''_j) + g(i''_j,i'_j)$.

Dacă $j \in J'$, atunci $g(i_j,i'_j) = 1$ şi putem scrie $g(i_j,i'_j) = g(i_j,i''_j) + g(i''_j,i'_j)$, unde h_o dintre simbolii i''_j

îi luăm egali cu i_j iar restul de $|J'|-h_o$ simboli îi luăm egali cu i'_j.

In sfîrşit dacă $j \in J''$, atunci $g(i_j,i'_j) = 0$, avem $i_j = i'_j$ şi putem scrie $g(i_j,i'_j) = g(i_j,i''_j) + g(i''_j,i'_j)$ luînd $i''_j = i_j = i'_j$.

Prin urmare:

$$\rho_g(p,q) = \sum_{j=1}^{n} g(i_j,i'_j) = \sum_{j=1}^{n} (g(i_j,i''_j) +$$

$$+ g(i''_j,i'_j)) = \sum_{j=1}^{n} g(i_j,i''_j) + \sum_{j=1}^{n} g(i''_j,i'_j) = \rho_g(p,r) +$$

$+ \rho_g(r,q)$ şi $\rho_g(p,r) = h$, iar $\rho_g(r,q)=k$, luînd $r = i''_1 i''_2 \ldots i''_n$.

Pentru simplitate, convenim să scrim ρ în loc de ρ_g, ori de cîte ori, g este o quasi-metrică pe I şi acest lucru nu duce la confuzii.

In continuare prezentăm cîteva quasi-metrice pe alfabetul $I = \{0,1,\ldots, n\}$.

<u>Exemplul III.1.2</u>. Fie

$$g(i,j) = \begin{cases} 0 & \text{dacă } i = j \\ 1 & \text{dacă } i \neq j. \end{cases}$$

Dacă $q \in [p]$, $p = i_1 \ldots i_n$ şi $q = i'_1 \ldots i'_n$, atunci $\rho_g(p,q) = |J|$, unde $J = \{j \mid j \in \{1,\ldots,n\}, i_j \neq i'_j\}$.

Prin urmare pentru coduri bloc, ρ_g este distanţa lui Hamming.

Evident g este o quasi metrică pe I, condiţia (III.1.2) fiind banal verificată.

<u>Exemplul III.1.3.</u> Fie $g(i,j) = |i-j|$. Putem presupune fără a restrînge generalitatea că dacă $|i-j|>1$, atunci $i-j > 1$.

E. te clar că g satisface la condiţiilei),ii) şi iii). Să arătăm că g este o quasi-metrică pe I. Fie deci $g(i,j)=i-j = h+k > 1$, $h,k \in \mathbb{N}^*$.

Atunci $i > h > o$ şi $i-(i-h) > o$, $(i-h)-j = k > o$. Avem $i-h \in I$ şi $g(i,j) = i-j = [i-(i-h)]+[(i-h)-j] = g(i,i-h) + g(i-h,j)$ şi $g(i,i-h) = h$ iar $g(i-h,j)=k$.

Exemplul III.1.4. Să considerăm că simbolul $0 \in I$ joacă un rol special, de "blanc" sau de simbol de "ştergere".

Definim aplicaţia $g: I \times I \to N$, prin:

$$g(i,j)= \begin{cases} 0 & \text{dacă } i = j \\ 1 & \text{dacă } i = 0, j \neq 0 \text{ sau } i \neq 0, j = 0 \\ 2 & \text{dacă } i \neq 0, j \neq 0 \text{ şi } i \neq j. \end{cases}$$

In această alegere a lui g o eroare contează cît două ştergeri.

Avem $g(i,j) \geqslant 0$ şi $g(i,j) = 0 \Leftrightarrow i = j$, deci are loc i).

Apoi $g(i,j) = g(j,i) \quad \forall\, i,j \in I$, deci are loc ii).

Să verificăm că are loc iii) deci $g(i,j) \leqslant g(i,i_1) + g(i_1,j)$.

Dacă $i = j$, atunci $g(i,j) = 0$ şi inegalitatea este banal verificată.

Dacă $i = 0, j \neq 0$ avem $g(i,j)=1$, iar

$$g(i,i_1)+g(i_1,j)= \begin{cases} 1 & \text{dacă } i_1 = 0 \\ 1 & \text{dacă } i_1 \neq 0,\ i_1 \neq j \\ 2 & \text{dacă } i_1 \neq 0,\ i_1 \neq j \ . \end{cases}$$

Deci şi în acest caz de verifică inegalitatea.

Apoi, dacă $i \neq 0$, $j \neq 0$, $i \neq j$, atunci $g(i,j) = 2$, iar

$$g(i,i_1)+g(i_1,j)= \begin{cases} 2 & \text{dacă } i_1 = 0 \\ 2 & \text{dacă } i_1 \neq 0, i_1 = i \text{ şi } i_1 \neq j \text{ sau } i_1 \neq i \text{ şi } i_1 = j \\ 4 & \text{dacă } i_1 \neq 0,\ i_1 \neq i \text{ şi } i_1 \neq j \ , \end{cases}$$

deci iar are loc inegalitatea.

Aplicaţia g este o quasi-metrică, întrucît are loc şi condiţia (III.1.2). Intr-adevăr pentru $g(i,j) \leq 1$, condiţia (III.1.2) se verifică banal. Fie deci $g(i,j) = 2$.

Atunci avem $g(i,j) = g(i,0) + g(0,j) = 1+1=2$ cu $g(i,0) = g(0,j) = 1$.

Exemplul III.1.5. Fie $I = \{0,1,2,3,4\}$ şi să definim aplicaţia $g : I \times I \longrightarrow N$ prin tabloul:

g	0	1	2	3	4
0	0	0	1	1	2
1	0	0	1	1	2
2	1	1	0	0	2
3	1	1	0	0	2
4	2	2	2	2	0

Deoarece $g(i,j) \geq 0$, $\forall i,j \in I$ este îndeplinită condiţia i). Din simetria tabloului faţă de diagonala principală, urmează $g(i,j) = g(j,i)$, $\forall i,j \in I$, deci are loc ii).

Să verificăm că $g(i,j) \leq g(i,i_1) + g(i_1,j)$, $\forall i,j,i_1 \in I$. Dacă $i = j$. inegalitatea este banal verificată;la fel dacă $i = 0, j = 1$; $i = 1$, $j = 0$; $i = 2, j = 3$; $i = 3, j = 2$. Apoi avem $g(0,2) = 1$, iar

$$g(0,i_1)+g(i_1,2) = \begin{cases} 1 & \text{dacă } i_1 = 0 \\ 1 & \text{dacă } i_1 = 1 \\ 1 & \text{dacă } i_1 = 2 \\ 2 & \text{dacă } i_1 = 3 \\ 4 & \text{dacă } i_1 = 4, \end{cases}$$

deci iar se verifică inegalitatea.

In mod analog se procedează şi în celelalte cazuri, de fiecare dată se constată că se verifică inegalitatea.

Vom arăta că nu are loc şi condiţia (III.1.2.), deci aplicaţia g nu este o quasi-metrică.

Avem $g(0,4) = 2 \neq g(0,i) + g(i,4)$ cu $g(0,i) = g(i,4) = 1$.

In continuare vom da cîteva exemple de coduri pe care le vom folosi apoi la verificarea unor proprietăţi speciale ale codurilor.

In toate cazurile vom lua $I = \{0,1\}$ şi $H = \{001, 1010, 01010\} = \{p_1, p_2, p_3\}$, cu $p_1 = 001$, $p_2 = 1010$ şi $p_3 = 01010$.

Exemplul III.1.6. Considerăm codul simplu (H, ι). Avem $\iota(p_1) = \{p_1\}$, $\iota(p_2) = \{p_2\}$ şi $\iota(p_3) = \{p_3\}$.

Exemplul III.1.7. Să definim indexarea $\theta: H \to N$, prin $\theta(p_1) = 2$, $\theta(p_2) = 1$ şi $\theta(p_3) = 0$, şi fie aplicaţia $g : I \times I \to N$, dată prin $g(0,0) = g(1,1) = 0$ şi $g(1,0) = g(0,1) = 1$. Se constată imediat că g este o quasi-metrică pe I. Atunci aplicaţia $\rho : H \times H \to N$, extinsă din aplicaţia g este dată în tabloul:

ρ	001	1010	01010
001	0	1	2
1010	1	0	4
01010	2	4	0

deoarece

$$\rho(001, 1010) = g(0,1) + g(0,0) + g(1,1) = 1,$$
$$\rho(001, 01010) = g(0,0) + g(0,1) + g(1,0) = 2,$$

iar

$$\rho(1010, 01010) = g(1,0) + g(0,1) + g(1,0) + g(0,1) = 4.$$

Să considerăm aplicaţia de calibrare

$\beta_\theta : H \to \mathcal{P}([H])$ dată prin $\beta_\theta(p) = s_{\theta(p)}(p; \rho)$.

Avem

$$s_{\theta(p_1)}(p_1; \rho) = \{p' \mid p' \in [p_1],\ \rho(p_1, p') \leq \theta(p_1)\},$$

deci

$$S_2(p_1;\rho) = \{p' \mid p' \in [p_1],\ \rho(p_1,p') \leq 2\} =$$
$$= \{001,\ 101,\ 011,\ 000,\ 111,\ 010,\ 100\}.$$

Apoi

$$S_1(p_2;\rho) = \{p' \mid p' \in [p_2],\ \rho(p_2,p') \leq 1\} =$$
$$= \{1010,\ 0010,\ 1110,\ 1000,\ 1011\}.$$

In sfîrşit

$$S_0(p_3;\rho) = \{p' \mid p' \in [p_3],\ \rho(p_3,p') \leq 0\} = \{01010\}.$$

Am construit astfel mulţimea calibrată (H, β_θ) cu

$$\beta_\theta(p) = S_{\theta(p)}(p;\rho).$$

Exemplul III.1.8. Fie θ indexarea şi g aplicaţia din exemplul precedent. Vom defini o aplicaţie de calibrare $\beta^\theta : H \longrightarrow \mathcal{P}([H])$ prin

$$\beta^\theta(p) = \{p' \mid p' \in [p],\ L(p,p') \leq \theta(p)\},$$

unde $L(p,p')$ se defineşte astfel

Fie $p = i_1 \ldots i_n$, $p' = i'_1 \ldots i'_n$ şi

$$D(p,p') = \{j \mid g(i_j, i'_j) \neq 0\}$$

Avem $D(p,p') \subset \{1,\ldots,n\}$ şi fie $j_1 = \min D(p,p')$, iar $j_2 = \max D(p,p')$, atunci $L(p,p') = 1 + (j_2 - j_1)$. Dacă $D(p,p') = \emptyset$, atunci $L(p,p') = 0$.

Fie $p = 001$. Atunci $[p] = \{001,\ 101,\ 011,\ 000,\ 111,\ 010,\ 100,\ 110\}$.

$D(001, 001) = \emptyset$; $D(001,101) = \{1\}$; $D(001, 011) = \{2\}$; $D(001, 000) = \{3\}$; $D(001, 111) = \{1,2\}$; $D(001, 010) = \{2,3\}$; $D(001, 100) = \{1,3\}$; $D(001, 110) = \{1,2,3\}$.

Prin urmare

$L(001, 001) = 0$, $L(001, 101) = L(001, 011) = L(001, 000) = 1$, $L(001, 111) = L(001, 010) = 2$, $L(001, 100) = L(001, 110) = 3$.

Intrucît $\theta(001) = 2$, avem:

$$\beta^\theta(001) = \{001,\ 101,\ 011,\ 000,\ 111,\ 010\}.$$

Apoi, fie p = 1010. Atunci [p] = {1010, 0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, 1000, 1001, 1011, 1100, 1101, 1110, 1111}.

D(1010, 1010) = ∅; D(1010, 0000) = {1,3}; D(1010, 0001) = {1,3,4};
D(1010, 0010) = {1}; D(1010, 0011) = {1,4}; D(1010, 0100) = {1,2,3};
D(1010, 0101) = {1,2,3,4}; D(1010, 0110) = {1,2}; D(1010, 0111) = {1,2,4};
D(1010, 1000) = {3}; D(1010, 1001) = {3,4}; D(1010, 1011) = {4};
D(1010, 1100) = {2,3}; D(1010, 1101) = {2,3,4}; D(1010, 1110) = {2};
D(1010, 1111) = {2,4}.

Prin urmare

L(1010, 1010) = 0, L(1010, 0010) = L(1010, 1011) = L(1010, 1110) = L(1010, 1000) = 1,
L(1010, 0110) = L(1010, 1001) = L(1010, 1100) = 2,
L(1010, 0000) = L(1010, 0100) = L(1010, 1101) = L(1010, 1111) = 3,
L(1010, 0001) = L(1010, 0011) = L(1010, 0101) = L(1010, 0111) = 4.

Cum $\theta(1010) = 1$, avem

$\beta^{\theta}(1010) = \{1010, 0010, 1011, 1110, 1000\}$.

In sfîrşit, fie p = 01010. Atunci [p] = {01010, 00000, 00001, 00010, 00011, 00100, 00101, 00110, 00111, 01000, 01001, 10100, 10101, 01011, 01100, 01101, 01110, 01111, 10000, 10001, 10010, 10011, 10110, 10111, 11000, 11001, 11010, 11011, 11100, 11101, 11110, 11111}.

Avem:

D(01010, 01010) = ∅;
D(01010, 00001) = {2,4,5};
D(01010, 00011) = {2,5};
D(01010, 00101) = {2,3,4,5};
D(01010, 00111) = {2,3,5};
D(01010, 01001) = {4,5};
D(01010, 00000) = {2,4};
D(01010, 00010) = {2};
D(01010, 00100) = {2,3,4};
D(01010, 00110) = {2,3};
D(01010, 01000) = {4};
D(01010, 10100) = {1,2,3,4};

$D(01010, 10101) = \{1,2,3,4,5\}$; $D(01010, 01011) = \{5\}$;

$D(01010, 01100) = \{3,4\}$; $D(01010, 01101) = \{3,4,5\}$;

$D(01010, 01110) = \{3\}$; $D(01010, 01111) = \{3,5\}$;

$D(01010, 10000) = \{1,2,4\}$; $D(01010, 10001) = \{1,2,4,5\}$;

$D(01010, 10010) = \{1,2\}$; $D(01010, 10011) = \{1,2,5\}$;

$D(01010, 10110) = \{1,2,3\}$; $D(01010, 10111) = \{1,2,3,5\}$;

$D(01010, 11000) = \{1,4\}$; $D(01010, 11001) = \{1,4,5\}$;

$D(01010, 11010) = \{1\}$; $D(01010, 11011) = \{1,5\}$

$D(01010, 11100) = \{1,3,4\}$; $D(01010, 11101) = \{1,3,4,5\}$;

$D(01010, 11110) = \{1,3\}$; $D(01010, 11111) = \{1,3,5\}$.

Prin urmare

$L(01010,01010) = 0$, $L(01010,01110) = L(01010,11010) =$

$= L(01010,00010) = L(01010,01000) = L(01010,01011) = 1$,

$L(01010,01001) = L(01010,01100) = L(01010,10010) = L(01010,00110)$

$= 2$,

$L(01010,10110) = L(01010,11110) = L(01010,00110) =$

$= L(01010,01101) = L(01010,01111) = L(01010,00000) = 3$,

$L(01010,00001) = L(01010,00011) = L(01010,00101) = L(01010,00111) =$

$= L(01010,11000) = L(01010,11100) = L(01010,10100) = L(01010,10000) =$

$= 4$,

$L(01010,10101) = L(01010,10001) = L(01010,10011) = L(01010,10111) =$

$= L(01010,11001) = L(01010,11011) = L(01010,11101) =$

$= L(01010,11111) = 5$.

Cum $\theta(01010) = 0$, avem

$$\beta^{\theta}(01010) = \{01010\}.$$

Exemplul III.19. Dacă în condiţiile exemplului precedent modificăm aplicaţia g şi anume cerem ca $g(0,0) = g(1,1) = g(1,0) = g(0,1) = 0$, atunci aplicaţia de calibrare corespunzătoare se schimbă. Astfel $\rho(p,p') = 0$, $\forall p,p' \in I^*$. Apoi $D(p,p') = \emptyset$,

$\forall p \in I^{\#}$ şi $p' \in [p]$, iar $l(p,p') = 1$.

Atunci $\beta^{\theta}(001) = [001]$, $\beta^{\theta}(1010) = [1010]$, iar $\beta^{\theta}(01010) = [01010]$.

Exemplul III.1.1o. In condiţiile din exemplul III.1.8, schimbăm aplicaţia de indexare θ , luînd $\theta_1(p_1) = 2$, $\theta_1(p_2) = 1$ şi $\theta_1(p_3) = 5$. Aplicaţia de calibrare corespunzătoare se modifică astfel:

$$\beta^{\theta_1}(001) = \beta^{\theta}(001), \quad \beta^{\theta_1}(1010) = \beta^{\theta}(1010),$$
$$\beta^{\theta_1}(01010) = [01010].$$

Observaţia III.1.9. Din exemplele III.1.8-1o rezultă că aplicaţiile de calibrare considerate depind de aplicaţia g şi de aplicaţia de indexare θ .

Observaţia III.1.1o. Deoarece în exemplul III.1.1, toate cuvintele din H sînt de lungimi diferite, mulţimea calibrata (H,β) din acel exemplu este un cod.

§ III.2. Şiruri de multimi calibrate

Fie I un alfabet finit şi $I^{\#}$ semigrupul liber generat de I .

Fie $p,q \in I^{\#}$ cu $\ell(p) \neq \ell(q)$. Există un cuvînt unic $r \in I^{\#}$ cu $p \in [q]r$ sau $q \in [p]r$. Vom pune $r = c(p,q)$.

Fie (H, β) şi (H_0, β_0) două mulţimi calibrate.

Definiţia III.2.1. Cuvintele $p \in H$ şi $p_0 \in H_0$, sînt compatibile dacă $\beta(p) \mid \beta_0(p_0) \neq \emptyset$

S-a notat prin $\beta(p) \mid \beta_0(p_0)$ cîtul complexelor $\beta(p)$ şi $\beta_0(p_0)$ (v.definiţia II.2.2.).

Observaţia III.2.1 Dacă cuvintele p şi p_0 sînt compatibile, atunci $\ell(p) \neq \ell(p_0)$ şi $\beta(p) \mid \beta_0(p_0) \in [r]$, unde $r = c(p,p_0)$.

Observaţia III.2.2 Dacă $\beta = \beta_0 = \iota$, atunci cuvintele $p \in H$ şi $p_0 \in H_0$ sînt compatibile dacă $p|p_0 \neq \emptyset$, iar $c(p,p_0) = p|p_0$.

Pornind de la mulţimile calibrate (H, β) şi (H_0, β_0) vom construi prin recurenţă un şir de mulţimi calibrate $\{(H_n, \beta_n) | n \in N\}$.

Fie mulţimea:

$$R_1(H, \beta ; H_0, \beta_0) = \{c(p,p_0) | p \in H, p_0 \in H_0, \beta(p) | \beta_0(p_0) \neq \emptyset\}.$$

Definim aplicaţia β_1 pe $R_1(H, \beta; H_0, \beta_0)$, punînd pentru $r_1 \in R_1(H, \beta; H_0, \beta_0)$,

$$\beta_1(r_1) = \bigcup \{ \beta(p) | \beta_0(p_0) | p \in H, p_0 \in H_0 \text{ şi } r_1 = c(p,p_0) \}.$$

Ţinînd seama de observaţia III.2.1, avem $\beta_1 : R_1(H, \beta ; H_0, \beta_0) \longrightarrow \mathcal{P}([R_1(H, \beta ; H_0, \beta_0)])$ deci β_1 este o aplicaţie de calibrare pe $R_1(H, \beta ; H_0, \beta_0)$.

Dacă $R_1(H, \beta ; H_0, \beta_0) = \emptyset$ atunci β_1 este aplicaţia vidă.

Vom nota $H_1 = R_1(H, \beta ; H_0, \beta_0)$ şi obţinem corespunzător mulţimea calibrată (H_1, β_1).

Repetăm construcţia precedentă pornind de la mulţimile calibrate (H, β) şi (H_1, β_1).

Să presupunem că a fost construită mulţimea calibrată (H_n, β_n).

Atunci punem

$$R_{n+1}(H, \beta ; H_0, \beta_0) = R_1(H, \beta ; H_n, \beta_n),$$

şi notăm $H_{n+1} = R_{n+1}(H, \beta ; H_0, \beta_0)$.

Avem deci

$$H_{n+1} = \{c(p,p_n) | p \in H, p_n \in H_n, \beta(p) | \beta_n(p_n) \neq \emptyset\}.$$

Definim apoi aplicaţia de calibrare β_{n+1} pe H_{n+1}, punînd

$$\beta_{n+1}(r_{n+1}) = \bigcup \{\beta(p) | \beta_n(p_n), p \in H, p_n \in H_n \text{ şi } r_{n+1} = c(p, p_n)\},$$

$\forall r_{n+1} \in H_{n+1}$.

Obţinem în acest fel mulţimea calibrată (H_{n+1}, β_{n+1}). Continuînd în acelaş mod obţinem şirul de mulţimi calibrate $\{(H_n, \beta_n) \mid n \in N\}$.

Observaţia III.2.3. Dacă există $n \in N^*$ cu $H_n = \emptyset$, atunci $H_{n+k} = \emptyset, \forall k \in N$.

Observaţia III.2.4. Să pornim de la mulţimile calibrate simple (H, ι) şi (H_0, ι). In acest caz, (H, ι) şi (H_0, ι) sînt coduri simple (v.observaţia III.1.2.).

Cuvintele $p \in H$ şi $p_0 \in H_0$ sînt compatibile dacă $p|p_0 \neq \emptyset$, iar $\{p\}|\{p_0\} = r = p|p_0$. Prin urmare

$$R_1(H, \iota ; H_0, \iota) = \{c(p,p_0) \mid p \in H, p_0 \in H_0, \{p\}|\{p_0\} \neq \emptyset\} =$$
$$= \{\{p\}|\{p_0\} \mid p \in H, p_0 \in H_0\} = H|H_0.$$

Apoi $\beta_1 : H|H_0 \longrightarrow \mathcal{P}([H|H_0])$, este dat de

$$\beta_1(r_1) = \bigcup\{\{p\}|\{p_0\} \mid p \in H, p_0 \in H_0 \text{ şi } r_1 \leq p|p_0\} = \{p|p_0\} =$$
$$= \{r_1\}, \forall r_1 \in H|H_0. \text{ Deci } \beta_1 = \iota .$$

Continuînd se obţine $\beta_n = \iota, \forall n \in N$ şi se regăsesc mulţimile $R_n(H, H_0)$ din observaţia II.2.5, considerate de Levenştein şi Riley.

Exemplul III.2.1 Fie (H, β) mulţimea calibrată din exemplul III.1.1. Să luăm $H_0 = H$ şi $\beta_0 = \beta$. Vom construi şirul de mulţimi calibrate $\{(H_n, \beta_n) \mid n \in N^*\}$ pornind de la mulţimile calibrate (H, β) şi (H, β).

Pentru a obţine mulţimea H_1, trebuiesc căutate perechile de cuvinte compatibile din H. Avem:

$\beta(001)|\beta(1010) = \{1\}$, iar $c(001, 1010) = 0$,

$\beta(001)|\beta(01010) = \{10, 01\}$, iar $c(001, 01010) = 10$,

$\beta(1010)|\beta(01010) = \{0\}$ iar $c(1010, 01010) = 0$.

Prin urmare $H_1 = R_1(H, \beta ; H, \beta) = \{0, 10\}$.

Apoi $\beta_1(0) = \beta(001)|\beta(1010) \cup \beta(1010)|\beta(01010) = \{0, 1\}$, iar

$\beta_1(10) = \beta(001)|\beta(01010) = \{10, 01\}$.

Am construit astfel mulţimea calibrată (H_1, β_1).

Pentru a obţine mulţimea H_2, trebuiesc căutate perechile de cuvinte compatibile (p, p_1) cu $p \in H$ şi $p_1 \in H_1$. Avem:

$\beta(001)|\beta_1(0) = \{01, 10, 00\}$, iar $c(001,0) = 01$,

$\beta(1010)|\beta_1(0) = \{010, 100, 001, 110, 101, 011\}$, iar $c(1010,0)=010$,

$\beta(01010)|\beta_1(0) = \{1010,1000,0100,0010, 0001,1100,1001,0110, 0101,0011\}$, iar $c(01010,0)=1010$,

$\beta(001)|\beta_1(10) = \{0\}$, iar $c(001,10) = 1$,

$\beta(1010)|\beta_1(10) = \{10, 01\}$, iar $c(1010,10)= 10$,

$\beta(01010)|\beta_1(10) = \{100,010,001\}$, iar $c(01010,10)=010$.

Astfel

$$H_2 = R_1(H, \beta; H_1, \beta_1) = \{01,010,1010,1,10\}.$$

Apoi

$\beta_2(01) = \{01, 10, 00\}$,

$\beta_2(010) = \{010, 100, 001, 110, 101, 011\}$,

$\beta_2(1010) = \{1010, 1000, 0100, 0010, 0001, 1100, 1001, 0110, 0101, 0011\}$,

$\beta_2(1) = \{0\}$,

$\beta_2(10) = \{10, 01\}$.

Am construit astfel mulţimea calibrată (H_2, β_2). Se continuă la fel. Mulţimile calibrate (H, β) şi (H_1, β_1) sînt coduri. Deoarece $\beta_2(01) \cap \beta_2(10) \neq \emptyset$, aplicaţia β_2 nu-i o aplicaţie de admisibilitate şi prin urmare mulţimea calibrată (H_2, β_2) nu-i cod.

Se observă că construcţia mulţimilor calibrate (H_n, β_n) cere un volum foarte mare de calcul.

Vom arăta că acest calcul se simplifică mult pentru mulţimile calibrate în care aplicaţia de calibrare este definită cu ajutorul β_3 - sferelor (v. observaţia III.1.6); deci, în particular

pentru coduri indexate (v.definiţia III.1.5). Aceasta, deoarece perechile de cuvinte compatibile pot fi caracterizate în funcţie de aplicaţiile ρ_g şi de indexarea θ .

În acest scop vom defini nişte aplicaţii pe mulţimile valibrate (H, β) şi (H_0, β_0).

Fie θ şi θ_0 indexări pe mulţimile finite H respectiv H_0, $g: I \times I \to N$ şi $\rho: I^* \times I^* \to N$ extinsă din g prin formula (III.1.1).

Introducerea aplicaţiilor:

a) $S : H \times H_0 \to N$, dată prin

$$S(p,p_0) = \begin{cases} \theta(p) & \text{dacă } \ell(p_0) < \ell(p) \\ \theta_0(p_0) & \text{dacă } \ell(p) < \ell(p_0) \\ \text{nedefinită} & \text{dacă } \ell(p) = \ell(p_0), \end{cases}$$

b) $F : H \times H_0 \to N$, dată prin:

$$F(p,p_0) = \theta(p) + \theta_0(p_0) - \rho(p,p_0)$$

şi

c) $M : H \times H_0 \to N$, dată prin

$$M(p,p_0) = \min\{S(p,p_0), F(p,p_0)\}.$$

Observaţia III.2.5. Aplicaţiile S şi M sînt definite numai pentru perechile $(p,p_0) \in H \times H_0$ cu $\ell(p) \neq \ell(p_0)$.

Apoi $M(p,p_0) \geq 0$, dacă şi numai dacă $F(p,p_0) \geq 0$ şi $S(p,p_0)$ există.

Teorema III.2.1. Avem $\beta_\theta(p) \mid \beta_{\theta_0}(p_0) \neq \emptyset$, dacă şi numai dacă $M(p,p_0) \geq 0$.

Demonstraţie. Fie $u \in \beta_\theta(p) \mid \beta_{\theta_0}(p_0)$, atunci $S(p,p_0)$ este definită deoarece $\ell(p) \neq \ell(p_0)$. Să presupunem că $\ell(p) < \ell(p_0)$.

Există atunci $p' \in \beta_\theta(p)$ şi $p'_0 \in \beta_{\theta_0}(p_0)$ astfel încît $p'_0 = p'u$, $\ell(p') = \ell(p)$, $\rho(p,p') \leq \theta(p)$ şi $\rho(p_0,p'_0) \leq \theta_0(p_0)$ (v.observaţia III.1.6). Atunci, ţinînd seama de proprieta-

tea 3) din teorema III.1.1 (pe care o aplicăm de două ori), obţinem:

$\rho(p,p_0) \leq \rho(p,p') + \rho(p',p_0) \leq \rho(p,p') + \rho(p',p'_0) + \rho(p'_0,p_0) \leq \theta(p) + 0 + \theta_0(p_0)$, deoarece $\rho(p',p'_0) = 0$ fiindcă $p' \in Pref\{p'_0\}$.

Avem, deci $F(p,p_0) = \theta(p) + \theta_0(p_0) - \rho(p,p_0) \geq 0$ şi prin urmare $M(p,p_0) \geq 0$.

Să presupunem acum că $M(p,p_0) \geq 0$ şi că $l(p) < l(p_0)$. Pentru ca $\beta_\theta(p) \mid \beta_{\theta_0}(p_0) \neq \emptyset$ este suficient să găsim un cuvînt $r \in \beta_\theta(p)$ cu $r \in Pref\rho\{p'_0\}$, unde $p'_0 \in \beta_{\theta_0}(p_0)$. Deoarece $M(p,p_0) \geq 0$, avem $F(p,p_0) \geq 0$ şi prin urmare $\rho(p,p_0) \leq \theta(p) + \theta_0(p_0)$. Din $l(p) < l(p_0)$ urmează existenţa unui $u \in I^* \setminus \{e\}$ cu $p_0 = p'u$ şi $p' \in [p]$. Atunci $\rho(p,p_0) = \rho(p,p') = \rho(pu,p') = \rho(pu,p'u) = \rho(pu,p_0) \leq \theta(p) + \theta_0(p_0)$.

Dacă $0 \leq \rho(p,p_0) \leq \theta(p)$ atunci avem şi $\rho(p,p') \leq \theta(p)$ şi deci $p' \in \beta_\theta(p)$. Dacă $0 \leq \rho(p,p_0) \leq \theta_0(p_0)$, atunci avem şi $\rho(pu,p_0) \leq \theta_0(p_0)$, deci $pu \in \beta_{\theta_0}(p_0)$. In ambele cazuri $\beta_\theta(p) \mid \beta_{\theta_0}(p_0) \neq \emptyset$.

Să presupunem deci că $1 < \rho(p,p_0) = \rho(p,p') = h + k \leq \theta(p) + \theta_0(p_0)$ cu $h,k \in N^*$ şi $h \leq \theta(p)$, iar $k \leq \theta_0(p_0)$. Atunci în baza observaţiei III.1.8, există $r \in [p]$ astfel încît $\rho(p,r) = h$ şi $\rho(r,p') = k$, sau $\rho(ru,p_0) = \rho(ru,p'u) = \rho(r,p') = k$. Ca atare, $r \in \beta_\theta(p)$, $ru \in \beta_{\theta_0}(p_0)$ şi $r \in Pref\{ru\}$. ■

Observaţia III.2.6. Verificarea compatibilităţii unei perechi de cuvinte (p,p_0) revine în baza teoremei precedente la calcularea lui $M(p,p_0)$.

Teorema III.2.2. Dacă $M(p,p_0) \geq 0$, atunci

$$\beta_\theta(p) \mid \beta_{\theta_0}(p_0) = \{r' \mid r' \in [\sigma(p,p_0)], \rho(r', \sigma(p,p_0)) \leq M(p,p_0)\}.$$

Demonstraţie. Fie $M(p,p_0) \geq 0$, $l(p) < l(p_0)$ şi $p_0 = p'r$ cu $p' \in [p]$ şi $\sigma(p,p_0) = r$. Prin urmare $\rho(p,p_0) \leq \theta(p) +$

$\cdot\ \hat{}(p_0)$.

Să presupunem $x' \in [x]$ și $\rho(x',x) \leqslant M(p,p_0)$ deci $x' \in \{x' \mid x' \in [o(p,p_0)]\ ,\ \rho(x',o(p,p_0)) \leqslant M(p,p_0)\}$. Dacă $p' \in \beta_\theta(p)$, atunci $\rho(p,p') \leqslant \theta(p)$ și deoarece $\rho(p'x',p_0) = \rho(p'x',p'x) = \rho(x',x) \leqslant M(p,p_0) \leqslant S(p,p_0) = \theta_0(p_0)$, urmează că $p'x' \in \beta_{\theta_0}(p_0)$, și deci $x' \in \beta_\theta(p) \mid \beta_{\theta_0}(p_0)$.

Dacă $p' \notin \beta_\theta(p)$, atunci $\rho(p,p') > \theta(p)$, iar $\theta(p) - \rho(p,p') = \theta(p) - \rho(p,p_0) < 0$ și $M(p,p_0) = \theta_0(p_0) + [\theta(p) - \rho(p,p_0)] < \theta_0(p) = S(p,p_0)$. Din $\rho(p,p') > \theta(p)$ urmează existența unui $p'' \in [p]$ astfel încît $\rho(p,p') = \rho(p,p'') + \rho(p'',p')$ și $\rho(p',p'') = \rho(p,p') - \theta(p)$, iar $\rho(p,p'') = \theta(p)$. Avem deci $p'' \in \beta_\theta(p)$ și fie $p'_0 = p''x'$. Vom arăta că $p'_0 \in \beta_{\theta_0}(p_0)$.

Într-adevăr, avem $\rho(p_0,p'_0) = \rho(p''x,p''x') = \rho(p'',p'') + \rho(x,x') = \rho(p,p') - \theta(p) + \rho(x,x') \leqslant \rho(p,p') - \theta(p) + M(p,p_0) = [\rho(p,p') - \theta(p)] + \theta_0(p_0) + [\theta(p) - \rho(p,p')] = \theta_0(p_0)$. Urmează că $p'_0 = p''x' \in \beta_{\theta_0}(p_0)$ și cum $p'' \in \beta_\theta(p)$, avem $x' \in \beta_\theta(p) \mid \beta_{\theta_0}(p_0)$.

Invers, fie $x' \in \beta_\theta(p) \mid \beta_{\theta_0}(p_0)$. Atunci există $p'_0 \in \beta_{\theta_0}(p_0)$ și $p'' \in \beta_\theta(p)$ astfel încît $p'_0 = p''x'$. Din $p'_0 \in \beta_{\theta_0}(p_0)$, urmează $0 \leqslant \rho(p_0,p'_0) = \rho(p''x,p''x') = \rho(p'',p'') + \rho(x,x') \leqslant \theta_0(p_0)$ și deci

$$\rho(x,x') \leqslant \theta_0(p_0) - \rho(p'',p''),$$

de unde avem și $\rho(x,x') \leqslant \theta(p) = S(p,p_0)$.

Dar,

$$\rho(p,p_0) = \rho(p,p') = \rho(p',p) \leqslant \rho(p',p'') + \rho(p'',p) \leqslant \rho(p',p'') + \theta(p),$$

deoarece $p'' \in \beta_\theta(p)$.

Prin urmare $\rho(p,p_0) - \theta(p) \leqslant \rho(p',p'')$ și avem:

$$\begin{aligned}\rho(x,x') &\leqslant \theta_0(p_0) - \rho(p',p'') \leqslant \\ &\leqslant \theta_0(p_0) - [\rho(p,p_0) - \theta(p)] = \\ &= \theta_0(p_0) + \theta(p) - \rho(p,p_0) = M(p,p_0).\end{aligned}$$

Avem $\rho(r,r') \leqslant \min\{S(p,p_0), F(p,p_0)\} = M(p,p_0)$.

Ca atare dacă $r' \in \beta_\theta(p) \mid \beta_{\theta_0}(p_0)$, atunci $r' \in [r]$, $r = c(p,p_0)$, iar $\rho(r,r') \leqslant M(p,p_0)$, deci $r' \in \{r' \mid r' \in [c(p,p_0)], \rho(r', c(p,p_0)) \leqslant M(p,p_0)\}$. ■

Observația III.2.7. Teorema precedentă arată că dacă $\beta_\theta(p) \mid \beta_{\theta_0}(p_0) \neq \emptyset$ și $r = c(p,p_0)$, atunci

$$\beta_\theta(p) \mid \beta_{\theta_0}(p_0) = S_{M(p,p_0)}(r, \rho),$$

adică $\beta_\theta(p) \mid \beta_{\theta_0}(p_0)$ este ρ - sfera cu centrul în r și de rază $M(p,p_0)$.

Teorema III.2.3. Fie (H, θ) și (H_0, θ_0) mulțimi indexate și $(H,\beta_\theta), (H_0, \beta_{\theta_0})$ mulțimile calibrate corespunzătoare. Dacă $R_1(H, \beta_\theta; H_0, \beta_{\theta_0}) = H_1 \neq \emptyset$, atunci există o indexare $\theta_1 : H_1 \longrightarrow \mathbb{N}$, astfel încît pentru orice $r \in H_1$, să avem $\beta_1(r) = \beta_{\theta_1}(r)$.

Demonstrație. Amintim că pentru orice $r \in R_1(H,\beta_\theta, H_0, \beta_{\theta_0})$ avem

$$\beta_1(r) = \bigcup\{\beta_\theta(p) \mid \beta_{\theta_0}(p_0) \mid p \in H, p_0 \in H_0 \text{ și } r = c(p,p_0)\},$$

prin urmare, ținînd seama de teorema precedentă și de observația III.2.7, avem:

$\beta_1(r) = \bigcup\{S_{M(p,p_0)}(r, \rho) \mid p \in H, p_0 \in H_0, r = c(p,p_0)\}$, deci $\beta_1(r)$ este o reuniune de ρ - sfere cu centrul în r, deci în fond o ρ-sferă cu centrul în r.

Vom defini indexarea $\theta_1 : H_1 \longrightarrow \mathbb{N}$ prin

$$\theta_1(r) = \max\{M(p,p_0) \mid p \in H, p_0 \in H_0, r = c(p,p_0)\},$$

pentru orice $r \in H_1$.

Avem $\beta_1(r) = S_{\theta_1(r)}(r, \rho) = \beta_{\theta_1}(r)$. ■

Consecința III.2.1. Dacă $\{(H_n, \beta_n) \mid n \in \mathbb{N}\}$ este șirul de mulțimi calibrate construite plecînd de la mulțimile calibrate (H, β_θ) și (H_0, β_{θ_0}), atunci dacă $H_n \neq \emptyset$, există o indexare

$\theta_1 : H_n \to N$, astfel încît $\beta_1(r) = \beta_{\theta_n}(r)$, pentru orice $r \in H_n$.

Exemplul III.2.2. Vom aplica rezultatele precedente pentru mulțimea indexată (H, θ) considerată în exemplul III.1.7. Avem $H = \{p_1, p_2, p_3\}$, $p_1=001$, $p_2=1010$, $p_3=01010$ și $\theta(p_1)=2$, $\theta(p_2) = 1$ și $\theta(p_3) = 0$. Iar $g(0,0) = g(1,1)=0$, și $g(1,0) = g(0,1) = 1$.

Să luăm $(H, \theta) = (H_0, \theta_0)$. În baza observațiilor III.2.6 și III.2.5 cuvintele $p,q \in H$ sînt compatibile dacă și numai dacă $\ell(p) \neq \ell(q)$ și $F(p,q) \geqslant 0$.

Avem $F(p_1,p_2)= \theta(p_1) + \theta(p_2) - \rho(p_1,p_2) = 2 + 1 - 1 \geqslant 0$ deoarece $\rho(p_1,p_2) = g(0,1) + g(0,0) + g(1,1) = 1$,

Apoi

$$F(p_1,p_3) = \theta(p_1) + \theta(p_3) - \rho(p_1,p_2) = 2 + 0 - 2 = 0,$$

deoarece

$$\rho(p_1,p_3)=g(0,0) + g(0,1) + g(1,0) = 2.$$

În sfîrșit

$$F(p_2,p_3) = \theta(p_2) + \theta(p_3) - \rho(p_2,p_3)=1+0 - 4 < 0$$

deoarece

$$\rho(p_2,p_3)=g(1,0)+g(0,1)+g(1,0)+g(0,1) = 4.$$

Prin urmare perechile de cuvinte (p_1,p_2) și (p_1,p_3) sînt compatibile:

Cum $c(p_1,p_2) = 0$, $c(p_1,p_3) = 10$, avem $H_1 = \{0,10\}$.

Să definim indexarea $\theta_1 : H_1 \to N$, conform cu teorema III.2.3. Pentru aceasta trebuie să calculăm $M(p_1,p_2)$ și $M(p_1,p_3)$. Avem:

$$M(p_1,p_2) = \min\{S(p_1,p_2), F(p_1,p_2)\} = \min\{\theta(p_2),2\} = 1,$$
$$M(p_1,p_3) = \min\{S(p_1,p_3), F(p_1,p_3)\} = \min\{\theta(p_3),3\} = 0.$$

Prin urmare

$$\theta_1(0) = 1, \text{ iar } \theta_1(10) = 0.$$

$\ldots : H_n \to N$, astfel încît $\beta_{\theta}(r) = \beta_{\theta_n}(r)$, pentru orice $r \in H_n$.

Exemplul III.2.2. Vom aplica rezultatele precedente pentru mulțimea indexată (H, θ) considerată în exemplul III.1.7. Avem $H = \{p_1, p_2, p_3\}$, p_1=001, p_2=1010, p_3=01010 și $\theta(p_1)$=2, $\theta(p_2) = 1$ și $\theta(p_3) = 0$. Iar $g(0,0) = g(1,1)$=0, și $g(1,0) = g(0,1) = 1$.

Să luăm $(H, \theta) = (H_0, \theta_0)$. În baza observațiilor III.2.6 și III.2.5 cuvintele $p, q \in H$ sînt compatibile dacă și numai dacă $\ell(p) \neq \ell(q)$ și $F(p,q) \geqslant 0$.

Avem $F(p_1,p_2) = \theta(p_1) + \theta(p_2) - \rho(p_1,p_2) = 2 + 1 - 1 \geqslant 0$ deoarece $\rho(p_1,p_2) = g(0,1) + g(0,0) + g(1,1) = 1$.

Apoi

$$F(p_1,p_3) = \theta(p_1) + \theta(p_3) - \rho(p_1,p_2) = 2 + 0 - 2 = 0,$$

deoarece

$$\rho(p_1,p_3) = g(0,0) + g(0,1) + g(1,0) = 2.$$

În sfîrșit

$$F(p_2,p_3) = \theta(p_2) + \theta(p_3) - \rho(p_2,p_3) = 1+0 - 4 < 0$$

deoarece

$$\rho(p_2,p_3) = g(1,0)+g(0,1)+g(1,0)+g(0,1) = 4.$$

Prin urmare perechile de cuvinte (p_1,p_2) și (p_1,p_3) sînt compatibile:

Cum $c(p_1,p_2) = 0$, $c(p_1,p_3) = 10$, avem $H_1 = \{0,10\}$.

Să definim indexarea $\theta_1 : H_1 \to N$, conform cu teorema III.2.3. Pentru aceasta trebuie să calculăm $M(p_1,p_2)$ și $M(p_1,p_3)$. Avem:

$$M(p_1,p_2) = \min\{S(p_1,p_2), F(p_1,p_2)\} = \min\{\theta(p_2), 2\} = 1,$$

$$M(p_1,p_3) = \min\{S(p_1,p_3), F(p_1,p_3)\} = \min\{\theta(p_3), 3\} = 0.$$

Prin urmare

$$\theta_1(0) = 1, \text{ iar } \theta_1(10) = 0.$$

Atunci $\beta_1(0) = \beta_{\theta_1}(0) = S_{\theta_1(0)}(0;\rho) = \{p \mid p \in [0], \rho(0,p) \leq \theta_1(0)\} = \{0,1\}$,

iar

$$\beta_1(10) = \{p \mid p \in [10],\ \rho(10,p) \leq 0\} = \{10\}$$

Am determinat pînă acum mulţimea calibrată (H_1, β_1).

Aplicăm acelaşi procedeu mulţimilor indexate (H, θ) şi (H_1, θ_1), pentru a determina mulţimea calibrată (H_2, β_2).

Să găsim mai întîi perechile de cuvinte compatibile (p,q) cu $p \in H$ şi $q \in H_1$. Avem:

$F(001,0) = \theta(001) + \theta_1(0) - \rho(001,0) = 2+1 = 3 \geq 0$,

$F(001,10) = \theta(001) + \theta_1(10) - \rho(001,10) = 2+0-1 = 1 \geq 0$,

$F(1010,0) = \theta(1010) + \theta_1(0) - \rho(1010,0) = 1 + 1 - 1 = 1 \geq 0$,

$F(1010,10) = \theta(1010) + \theta_1(10) - \rho(1010,10) = 1 \geq 0$,

$F(01010,0) = \theta(01010) + \theta_1(0) - \rho(01010,0) = 1 \geq 0$,

$F(01010,10) = \theta(01010) + \theta_1(10) - (01010,10) = -2 < 0$.

Prin urmare:

$H_2 = \{c(001,0), c(001,10), c(1010,0), c(1010,10), c(01010,0)\} = \{01, 1, 010, 10, 1010\}$.

Să definim acum indexarea $\theta_2 : H_2 \to N$.

Deoarece pentru orice cuvînt $r \in H_2$ există o singură pereche de cuvinte compatibile $p \in H$, $q \in H_2$ cu $r = c(p,q)$, avem $\theta_2(r) = M(p,q)$.

Deci

$\theta_2(01) = M(001,0) = \min\{2,3\} = 2$,

$\theta_2(1) = M(001,10) = \min\{2,1\} = 1$,

$\theta_2(010) = M(1010,0) = \min\{1,1\} = 1$,

$\theta_2(10) = M(1010,10) = \min\{1,1\} = 1$,

$\theta_2(1010) = M(01010,0) = \min\{0,1\} = 0$.

Iar

$\beta_2(01) = \{01, 11, 00, 10\}$, $\beta_2(1) = \{1, 0\}$,

$\beta_2(010) = \{010, 110, 000, 011\}$, $\beta_2(10) = \{10, 11, 00\}$,

şi $\beta_2(1010) = \{1010\}$.

Se continuă la fel. Se observă că mulţimea calibrată (H_2, β_2) nu-i cod, deoarece $\beta_2(01) \cap \beta_2(10) \neq \emptyset$.

Vom stabili în sfîrşit, legătura dintre şirul de mulţimi calibrate asociate mulţimilor calibrate (H, β) şi (H_0, β_0) şi şirul mulţimilor calibrate asociat mulţumirilor calibrate extinse $(\beta(H), \iota)$ şi $(\beta_0(H_0), \iota)$.

Teorema III.2.4. Fie (H, β) şi (H_0, β_0) mulţimi calibrate.

Atunci

$$R_1(\beta(H), \iota ; \beta_0(H_0), \iota) = \beta_1(R_1(H, \beta ; H_0, \beta_0)).$$

Demonstraţie. Deoarece $R_1(\beta(H), \iota ; \beta_0(H_0), \iota) = \beta(H) \mid \beta_0(H_0) = \cup\{\beta(p) \mid \beta_0(p_0) \mid p \in H, p_0 \in H_0\}$, avem de arătat că:

$$\cup\{\beta(p) \mid \beta_0(p_0) \mid p \in H, p_0 \in H_0\} = \cup\{\beta_1(r) \mid r \in R_1(H, \beta ; H_0, \beta_0)\}.$$

Prin definiţie $\beta_1(r) = \cup\{\beta(p) \mid \beta_0(p_0) \mid p \in H, p_0 \in H_0$ şi $r = c(p, p_0)\}$ şi deci

$$\cup\{\beta_1(r) \mid r \in R_1(H, \beta ; H_0, \beta_0)\} \subseteq \cup\{\beta(p) \mid \beta_0(p_0) \mid p \in H, p_0 \in H_0\}.$$

Invers, fie $r' \in \beta(p) \mid \beta_0(p_0)$. Atunci $\beta(p) \mid \beta_0(p_0) \neq \emptyset$, prin urmare $\ell(p) \neq \ell(p_0)$ şi deci există $r \in R_1(H, \beta ; H_0, \beta_0)$ cu $c(p, p_0) = r$. Urmează $\beta(p) \mid \beta_0(p_0) \subset \beta_1(r)$ şi prin urmare

$$\cup\{\beta(p) \mid \beta_0(p_0) \mid p \in H, p_0 \in H_0\} \subseteq \cup\{\beta_1(r) \mid r \in R_1(H, \beta ; H_0, \beta_0)\}. \blacksquare$$

Teorema III.2.5.

$$R_n(\beta(H), \iota ; \beta_0(H_0), \iota) = \beta_n(R_n(H, \beta ; H_0, \beta_0)), \quad \forall n \in \mathbb{N}^*.$$

Demonstraţie

Vom proceda prin inducţie după n. Pentru $n = 1$, afirmaţia este adevărată în baza teoremei III.2.4. Să presupunem că proprie-

tatea are loc pentru n şi trecem la n+1.

Avem

$$R_{n+1}(\beta(H),\iota;\beta_0(H_0),\iota) = R_1(\beta(H),\iota; R_n(\beta(H),\iota;\beta_0(H_0),\iota),\iota).$$

Dar, prin ipoteza inductivă

$$R_n(\beta(H),\iota;\beta_0(H_0),\iota) = \beta_n(R_n(H,\beta;H_0,\beta_0))$$ şi deci

$$R_{n+1}(\beta(H),\iota;\beta_0(H_0),\iota) = R_1(\beta(H),\iota;\beta_n(R_n(H,\beta;H_0,\beta_0)),\iota) =$$

$$= R_1(\beta(H),\iota;\beta_n(H_n),\iota) = \beta_{n+1}(R_1(H,\beta;H_n,\beta_n)) =$$

$$\beta_{n+1}(R_{n+1}(H,\beta;H_0,\beta_0)).$$

Am aplicat iar teorema III.2.4 pentru mulţimile calibrate (H,β) şi (H_n,β_n) şi am ţinut seama de definiţia lui β_{n+1} şi a lui $R_1(H,\beta;H_n,\beta_n)$. ■

Observaţia III.2.8. Să presupunem că se pleacă de la mulţimile calibrate (H,β) şi (H_0,β_0) şi se formează mulţimea calibrată $(R_n(H,\beta;H_0,\beta_0),\beta_n)$ şi apoi mulţimea calibrată extinsă $(\beta_n(R_n(H,\beta;H_0,\beta_0)),\iota)$.

Apoi se pleacă de la mulţimile calibrate extinse $(\beta(H),\iota)$ şi $(\beta_0(H_0),\iota)$ şi se formează mulţimea calibrată simplă $(R_n(\beta(H),\iota;\beta_0(H_0),\iota),\iota)$, atunci teoremele precedente arată că

$$(\beta_n(R_n(H,\beta;H_0,\beta_0)),\iota) = (R_n(\beta(H),\iota;\beta_0(H_0),\iota),\iota).$$

§ III.3. Coduri corectoare.

Se ştie că un cod (H,α) este corector dacă $m_1,m_2 \in H^*$ şi $\alpha(m_1)\cap\alpha(m_2)\neq\emptyset$, atunci $m_1 = m_2$.

Intrucît proprietatea unui cod de a fi corector este o proprietate extensibilă (v.observaţia I.3.2) urmează că din teorema II.2.5 se poate obţine o caracterizare pentru coduri (H,α) corectoare şi anume, codul (H,α) este corector dacă şi numai dacă $\alpha(H)\cap R_n(\alpha(H)) = \emptyset$, $\forall n\geq 1$.

Verificarea pentru un cod (H, α)dacă este corector folosind caracterizarea precedentă, este legată de greutăţi mari de calcul întrucît chiar dacă H este o mulţime cu un număr mic de elemente, $\alpha(H)$ poate avea foarte multe elemente.

De aceea sînt utile alte caracterizări pentru coduri corectoare, folosind mulţimi calibrate, care sînt date în:

Teorema III.3.1. Fie (H, α) un cod. Următoarele afirmaţii sînt echivalente:

C_1) Codul (H, α) este corector

C_2) $\alpha(H) \cap \alpha_n(R_n(H, \alpha; H, \alpha)) = \emptyset$, pentru $\forall n \in N^*$.

C_3) Pentru orice $n \in N^*$, dacă $r \in R_n(H, \alpha; H, \alpha)$ şi $p \in H$, atunci $\alpha(p) \cap \alpha_n(r) = \emptyset$.

Demonstraţie. Echivalenţa C1)$\Leftrightarrow$C2) urmează din teorema II.2.5, aplicată codului simplu extins $(\alpha(H), \iota)$ şi din teorema III.2.5.

Echivalenţa C2)$\Leftrightarrow$C3) rezultă din faptul că

$$\alpha(H) \cap \alpha_n(R_n(H, \alpha; H, \alpha)) = \left[\bigcup_{p \in H} \alpha(p)\right] \cap \left[\bigcup \left\{\alpha_n(r) \mid r \in R_n(H, \alpha; H, \alpha)\right\}\right] = \bigcup \left[\alpha(p) \cap \alpha_n(r)\right] . \blacksquare$$

Observaţia III.3.1. Dacă codul (H, α) este un cod indexat (v. definiţia III.1.5.), deci $\alpha = \alpha_\theta$ unde θ este o indexare $\theta : H \to N$, atunci condiţia C3) din teorema precedentă se poate scrie sub forma:

C3') Pentru orice $n \in N^*$, dacă $r \in R_n(H, \alpha; H, \alpha)$ şi $p \in H$, atunci $\rho(p, r) > \theta(p) + \theta_n(r)$, unde θ_n este indexarea pe H_n.

Exemplul III.3.1. Fie $I = \{0, 1\}$ şi $H = \{001, 1010, 01010\}$; codul simplu (H, ι) este corector căci $R_1(H, \iota; H, \iota) = \emptyset$.

Exemplul III.3.2. Fie codul (H, β) considerat în exemplul III.1.1. (deoarece cele trei cuvinte din H sînt de lungimi diferite, aplicaţia de calibrare β este o aplicaţie de admisibilitate.)

Vom verifica proprietatea de corectare a codului folosind echivalenţa C1)⟺ C2) din teorema III.3.1.

Folosind rezultatele din exemplul III.2.1, avem $H_1 = \{0, 10\}$, $\beta_1(0) = \{0,1\}$, iar $\beta_1(10) = \{10,01\}$.

Apoi $H_2 = \{01, 010, 1010, 1, 10\}$. Deoarece $\beta(H) \cap H_2 \neq \emptyset$, codul (H, β) nu-i corector.

Exemplul III.2.2. Să considerăm codul (H, β_0) construit în exemplul III.1.7. Să construim şirul de mulţimi calibrate (H_n, β_n).

Să căutăm perechile de cuvinte compatibile din H. Avem

$\beta_0(001) \mid \beta_0(1010) = \{0\}$, iar $c(001,1010) = 0$,

$\beta_0(001) \mid \beta_0(01010) = \{10\}$, iar $c(001,01010) = 10$,

$\beta_0(1010) \mid \beta_0(01010) = \emptyset$.

Prin urmare $H_1 = R_1(H, \beta_0 ; H, \beta_0) = \{0, 10\}$.

Apoi

$\beta_1(0) = \{0\}$, iar $\beta_1(10) = \{10\}$.

Am construit astfel mulţimea calibrată (H_1, β_1).

Pentru a obţine mulţimea H_2, trebuiesc căutate perechile de cuvinte compatibile (p, p_1) cu $p \in H$ şi $p_1 \in H_1$. Avem :

$\beta_0(001) \mid \beta_1(0) = \{01, 11, 00, 10\}$, iar $c(001,0) = 01$,

$\beta_0(1010) \mid \beta_1(0) = \{010\}$, iar $c(1010,0) = 010$,

$\beta_0(01010) \mid \beta_1(0) = \{1010\}$, iar $c(01010,0) = 1010$,

$\beta_0(001) \mid \beta_1(10) = \{1, 0\}$, iar $c(001,10) = 1$,

$\beta_0(1010) \mid \beta_1(10) = \{10, 00, 11\}$, iar $c(1010,10) = 10$,

$\beta_0(01010) \mid \beta_1(10) = \emptyset$.

Astfel $H_2 = R_1(H, \beta_0 ; H_1, \beta_1) = \{01, 010, 1010, 1, 10\}$.

Deoarece $R_1(H, \beta_0 ; H_1, \beta_1) \cap H \neq \emptyset$ codul (H, β_0) nu-i corector.

§ III.4.Coduri decodabile

Intrucît proprietatea unui cod de a fi decodabil este o proprietate extensibilă (v.teorema I.3.2.) urmează că din teorema II.4.3. se poate obţine o caracterizare pentru coduri decodabile şi anume codul (H,α) este decodabil dacă şi numai daca există $n_0 \in N^*$, astfel încît $R_{n_0}(\alpha(H)) = \emptyset$.

Următoarea teoremă dă o caracterizare a codurilor decodabile, folosind mulţimile calibrate. Astfel are loc :

Teorema III.4.1 Codul (H,α) este decodabil dacă şi numai dacă estecorector şi $R_{n_0}(H,\alpha ; H,\alpha) = \emptyset$ pentru un $n_0 \geq 1$.

Demonstraţie. In baza teoremei III.2.5 şi a faptului că proprietate unui cod de a fi decodabil este o proprietate extensibilă, urmează că (H,α) este un cod decodabil dacă şi numai dacă este corector şi $\alpha_{n_0}(R_{n_0}(H,\alpha ; H,\alpha)) = \emptyset$ pentru un $n_0 \geq 1$. Dar $\alpha_{n_0}(R_{n_0}(H,\alpha ; H,\alpha)) = \emptyset$ dacă şi numai dacă $R_{n_0}(H,\alpha ; H,\alpha) = \emptyset$. ∎

Exemplul III.4.1. Fie $I = \{0,1\}$ şi $H = \{001, 1010, 01010\}$. Codul simplu (H,ι) este decodabil deoarece $R_1(H,\iota ; H,\iota) = \emptyset$.

Exemplul III.4.2. [Hartnett [30]] .Fie $I = \{0,1\}$ şi $H = \{010110, 01001101\}$. Fie indexarea $\theta : H \to N$, dată prin $\theta(010110) = \theta(01001101) = 1$. Să calculăm aplicaţia de calibrare corespunzătoare. Fie încă $g(0,0) = g(1,1) = 0$ şi $g(1,0) = 1$. Atunci aplicaţia $\rho : H \times H \to N$, extinsă din aplicaţia g este dată în tabloul

ρ	010110	01001101
010110	0	2
01001101	2	0

Atunci

$$\beta_\theta(p) = S_{\theta(p)}(p;\rho) = \{p' \mid p' \in [p] \ , \rho(p',p) < \theta(p)\} \ .$$

Prin urmare

$$\beta_\theta(010110) = \{010110, 110110, 000110, 011110, 010010, 010100, 010111\},$$

iar

$$\beta_\theta(01001101) = \{01001101, 11001101, 00001101, 01101101, 01011101, 01000101, 01001001, 01001111, 01001100\}.$$

Vom verifica compatibilitatea perechilor de cuvinte folosind teorema III.2.1.

Avem $\ell(010110) \neq \ell(01001101)$ şi $F(010110, 01001101) = \theta(010110) + \theta(01001101) - \rho(010110, 01001101) = 1 + 1 - 2 \geq 0$ şi deci cuvintele 010110 şi 01001101 sînt compatibile. Avem

$$H_1 = R_1(H, \beta_\theta; H, \beta_\theta) = \{c(010110, 01001101)\} = \{01\}$$

Apoi $\theta_1(01) = M(010110, 01001101) = \min\{S(010110, 01001101), F(010110, 01001101)\} = 0$.

Pentru a determina mulţimea H_2, verificăm compatibilitatea cuvintelor 01 cu 010110 şi 01001101.

Avem $\ell(01) \neq \ell(010110)$, $F(010110, 01) = \theta(010110) + \theta_1(01) - \rho(010110, 01) = 1 + 0 - 0 = 1 \geq 0$, deci cuvintele 01 şi 010110 sînt compatibile, iar $c(010110, 01) = 0110$.

Apoi $\ell(01001101) \neq \ell(02)$, iar $F(01001101, 01) = \theta(01001101) + \theta_1(01) - \rho(01001101) = 1 + 0 - 0 = 1 \geq 0$ şi $c(01001101, 01) = 001101$. Prin urmare $H_2 = \{0110, 001101\}$.

Apoi

$$\theta_2(0110) = M(010110, 01) = \min\{1, 1\} = 1,$$

$$\theta_2(001101) = M(01001101, 01) = \min\{1, 1\} = 1.$$

Să găsim acum mulţimea H_3. Deoarece $\ell(010110) = \ell(001101)$, cuvintele 010110 şi 00110 nu sînt compatibile. Rămîne de calculat:

$F(010110,0110) = \theta(010110)+\theta_2(0110)-\rho(010110,0110)=1+1-2\geq 0,$

$F(01001101,0110)=\theta(01001101)+\theta_2(0110)-\rho(01001101,0110)=$

$=1+1-1=1\geq 0,$

$F(01001101,001101) = \theta(01001101)+\theta_2(001101)-\rho(01001101,001101)=$

$=1+1-4<0.$

Avem

$c(010110,0110) = 10$, iar $c(01001101,0110) = 1101$ deci

$H_3=\{10,1101\}$. Apoi $\theta_3(10) = \min\{1,0\}= 0$, iar $\theta_3(1101) =$

$=\min\{1,1\}= 1.$

Să determinăm mulțimea H_4. Avem

$F(010110,10) = 1+0-\rho(010110,10) = 1-2<0,$

$F(010110,1101) = 1+1-\rho(010110,1101) = 1+1-1=1\geq 0,$

$F(01001101,10) = 1+0-2<0,$

$F(01001101,1101) = 1+1-2\geq 0,$

Deoarece $c(010110,1101) = 10$ și $c(01001101,1101)=1101$,

avem $H_4 =\{10,1101\}$. Apoi $\theta_4(10) = \min\{1,1\}= 1$, iar $\theta_4(1101) =$

$= \min\{1,0\}= 0.$

Să găsim acum mulțimea indexată (H_5,θ_5).

Avem:

$F(010110,10) = 1+1-2\geq 0$, iar $c(010110,10)=0110$,

$F(010110,1101)= 1+0-1\geq 0$, iar $c(010110,1101)=10$,

$F(01001101,10)= 1+1-2\geq 0$, iar $c(01001101,10)=001101$,

$F(01001101,1101)=1+0-2<0$

Prin urmare $H_5 =\{10,0110, 001101\}$. Obținem $\theta_5(10)=$

$= \theta_5(0110) = \theta_5(001101) = 0.$

Continuînd la fel obținem:

$F(010110,101 = 1+0-2<0,$

$F(010110,0110)=1+0-1\geq 0$, iar $c(010110,0110) = 10$,

$F(01001101,10) = 1+0-2<0,$

$F(01001101,0110)=1+0-2<0,$

$F(01001101,001101) = 1+0-4<0,$

Avem deci $H_6 =\{10\}$, iar $\theta_6(10) = 0$.

Apoi

$F(010110,10) < 0$, iar $F(01001101,10) < 0$.

Deci $H_7 = \emptyset = R_7(H,\alpha_0 ; H,\alpha_6)$.

Rezultatele obținute le sintetizăm în tabloul următor:

H	θ	H_1	θ_1	H_2	θ_2	H_3	θ_3	H_4	θ_4	H_5	θ_5	H_6	θ_6	H_7
010110	1	01	0	0110	1	10	0	10	1	10	0	10	0	
01001101	1			001101	1	1101	1	1101	0	0110	0			
										001101	0			

Se verifică imediat că $\alpha_\theta(H) \cap H_j = \emptyset$, $j=\overline{1,6}$, prin urmare $\alpha_\theta(H) \cap H_j = \emptyset$, $\forall j \in \mathbb{N}^*$. Deoarece avem şi $R_7(H, \alpha_\theta; H, \alpha_\theta) = \emptyset$, codul (H, α_θ) este decodabil.

§ III.5. Coduri sincronizabile

Deoarece proprietatea unui cod de a fi sincronizabil este o proprietate extensibilă (v.teorema I.3.5.), din teorema II.5.1 se poate obţine o caracterizare pentru coduri sincronizabile şi anume codul (H, α) este sincronizabil dacă şi numai dacă este corector şi $R_{n_0}(\alpha(H); \text{Sufp}\,\alpha(H)) = \emptyset$ pentru un $n_0 \geq 1$.

Folosind mulţimile calibrate se pot obţine caracterizări pentru coduri sincronizabile, mai utile pentru aplicaţii. Are loc:

Teorema III.5.1. Codul (H, α) este sincronizabil dacă şi numai dacă este corector şi $R_{n_0}(H, \alpha; \text{Sufp}\,\alpha(H), \iota) = \emptyset$ pentru un $n_0 \geq 1$.

Demonstraţie. Putem scrie $R_{n_0}(\alpha(H), \text{Sufp}\,\alpha(H))$ ca $R_{n_0}(\alpha(H); \iota(\text{Sufp}\,\alpha(H)))$ şi să aplicăm teorema III.2.5. mulţimilor calibrate (H, α) şi $(\text{Sufp}\,H, \iota)$. Atunci $R_{n_0}(\alpha(H), \iota(\text{Sufp}\,\alpha(H))) = \alpha_{n_0}(R_{n_0}(H, \alpha; \text{SufpH}, \iota))$. Avem $\alpha_{n_0}(R_{n_0}(H, \alpha; \text{Sufp}\,\alpha(H), \iota)) = \emptyset$ dacă şi numai dacă $R_{n_0}(H, \alpha; \text{Sufp}\,\alpha(H), \iota)) = \emptyset$. ■

Observaţia III.5.1. In teorema precedentă trebuie de calculat mulţimile $R_{n_0}(H, \alpha; \text{Sufp}\,\alpha(H), \iota)$ ceea ce implică mulţimile H şi $\alpha(H)$. Se pot da caracterizări pentru coduri sincronizabile în care calculele să fie legate de mulţimi care implică numai mulţimea H.

In prealabil este necesară:

Teorema III.5.2. Fie (A, ι), (B, ι) şi (C, ι) mulţimi calibrate simple. Atunci $(B \cup C, \iota)$ este o mulţime calibrată simplă şi pentru orice $n \in \mathbb{N}^*$,

(III.5.1) $R_n(A, B \cup C) = R_n(A,B) \cup R_n(A,C)$.

Demonstrație. Mai întîi este clar că $(B \cup C, \iota)$ este o mulțime calibrată. Vom demonstra egalitatea (III.5.1) prin inducție după n. Pentru n =1, avem $R_1(A,B \cup C) = A|B \cup C =$ $= A|B \cup A|C = R_1(A,B) | R_1(A,C)$ și egalitatea se verifică. Se presupune, că este adevărată pentru n = k. Atunci

$$R_{k+1}(A, B \cup C) = R_1(A,R_k(A, B \cup C)) = R_1(A,R_k(A,B) \cup R_k(A,C)) =$$
$$= R_1(A,R_k(A,B)) \cup R_1(A,R_k(A,C)) = R_{k+1}(A,B) \cup R_{k+1}(A,C). \blacksquare$$

Să notăm cu $T(\alpha(H)) = \alpha(H) \cup Sufp\,\alpha(H)$.

Teorema III.5.3. Codul (H, α) este sincronizabil dacă și numai dacă este corector și $R_{n_o}(\alpha(H), \iota; T(\alpha(H)), \iota) = \emptyset$, pentru un $n_o \geq 1$.

Demonstrație. In baza teoremei precedente, pentru orice $n \in N^*$, avem:

$$R_n(\alpha(H), T(\alpha(H)) = R_n(\alpha(H), \alpha(H) \cup Sufp(H)) =$$
$$= R_n(\alpha(H), \alpha(H)) \cup R_n(\alpha(H), Sufp\,\alpha(H)).$$

Prin urmare, dacă există $n_o \in N^*$, $R_{n_o}(\alpha(H), T(\alpha(H))) = \rho$ și codul (H, α) este corector, atunci $R_{n_o}(\alpha(H), Sufp\,\alpha(H)) = \emptyset$ și deci codul (H, α) este sincronizabil.

Invers, dacă codul (H, α) este sincronizabil, atunci (H, α) este corector și există $n_1 \in N^*$ cu $R_{n_1}(\alpha(H), Sufp\,\alpha(H)) = \emptyset$. Dar codul (H, α) fiind sincronizabil este și decodabil (v. teorema I.3.7) și deci există $n_2 \in N^*$ cu $R_{n_2}(\alpha(H), \alpha(H)) = \emptyset$.

Luînd $n_o = \max\{n_1, n_2\}$, avem:

$$\emptyset = R_{n_o}(\alpha(H), \alpha(H)) \cup R_{n_o}(\alpha(H), Sufp\,\alpha(H)) = R_{n_o}(\alpha(H), T(\alpha(H))). \blacksquare$$

Vom defini acum o aplicație de calibrare α_T pe $T(H) = H \cup$ $\cup SufpH$, astfel încît $T(\alpha(H)) = \alpha_T(T(H))$.

Pentru $p \in T(A)$ definim

$$\alpha_T(p) \quad \bigcup \{[q] \cap T(\alpha(p)) \mid q \in T(\{p\})\}.$$

Vom spune că α_T este <u>calibrarea</u> pe $T(H)$ <u>indusă</u> de α iar $(T(H),\alpha_T)$ este <u>mulțimea calibrată</u> indusă de (H,α).

<u>Teorema III.5.4</u>. Avem:

(1) $T(\alpha(H)) = \bigcup\{T(\alpha(p)) \mid p \in H\}$,

(2) $T(\alpha(H)) = \alpha_T(T(H))$.

<u>Demonstrație</u>. Să verificăm afirmația (1). Deoarece $\alpha(p) \subset \alpha(H)$ pentru $\forall p \in H$, avem $T(\alpha(p)) \subset T(\alpha(H))$ și deci $\bigcup\{T(\alpha(p)) \mid p \in H\} \subseteq T(\alpha(H))$. Invers, fie $q \in T(\alpha(H))$, atunci există un cuvînt $q' \in \alpha(H)$ cu $q' \leq uq$. Cum $\alpha(p_1) \cap \alpha(p_2) = \emptyset$ dacă $p_1 \neq p_2$ există un $p \in H$ cu $q' \in \alpha(p)$. Atunci $q \in T(\alpha(p))$ și deci $T(\alpha(H)) \subseteq \bigcup\{T(\alpha(p)) \mid p \in H\}$.

Să demonstrăm afirmația (2). Fie $q' \in \alpha(q)$. Atunci $q' \in T(\alpha(p))$ pentru un $p \in H$, și deci $q' \in T(\alpha(H))$. Astfel $\alpha_T(q) \subseteq T(\alpha(H))$, de unde $\alpha_T(\alpha(H)) = \bigcup\{\alpha_T(q) \mid q \in T(H)\} \subseteq T(\alpha(H))$. Invers, dacă $q' \in T(\alpha(H))$, atunci $q' \in T(\alpha(p))$ cu $p \in H$ și $p = u q'$ cu $\ell(q') = \ell(q)$. Dar atunci $q' \in \alpha_T(q)$ și astfel $T(\alpha(H)) \subset \subset \alpha_T(T(H))$. ■

Următoarea teoremă oferă un algoritm pentru verificarea proprietății de sincronizare a unui cod.

<u>Teorema III.5.5</u>. Un cod (H,α) este sincronizabil dacă și numai dacă este corector și există $n \in \mathbb{N}^*$ astfel încît $R_n(H,\alpha;\ T(H),\alpha_T) = \emptyset$.

<u>Demonstrație</u>. În baza teoremelor III.5.4(2) și III.5.3. codul (H,α) este sincronizabil dacă și numai dacă codul (H,α) este corector și există $n_0 \in \mathbb{N}^*$ cu $R_{n_0}(\alpha(H),\iota;\alpha_T(T(H)),\iota) = \emptyset$. În virtutea teoremei III.2.5. putem înlocui $R_{n_0}(\alpha(H),\iota;\ \alpha(T(H)),\iota)$ prin $\alpha_{n_0}(R_{n_0}(H,\alpha;\ T(H),\alpha_T))$. Atunci $\alpha_{n_0}(R_{n_0}(H,\alpha;\ T(H),\alpha_T)) = \emptyset$, dacă și numai dacă $R_{n_0}(H,\alpha;\ T(H),\alpha_T) = \emptyset$.

Să considerăm acum cazul mulțimilor indexate (H,θ) (v.definiția III.1.4.).

Vom introduce aplicaţiile m: $T(H) \dashrightarrow N$, dată pentru orice $q \in T(H)$ prin $m(q) = \min\{\rho(q,q') \mid q' \in [q]\}$ şi $F_T : T(H) \times H \dashrightarrow N$, dată prin

$$F_T(q,p) = \min\{m(q), \Theta(p)\}, \quad \forall (q,p) \in T(H) \times H.$$

Apoi fie $\Theta_T(q) = \max\{F_T(q,p) \mid p \in H \text{ şi } q \in T(\{p\})\}$.

Deoarece pentru orice $q \in T(H)$ există un $p \in H$ cu $uq = p$ avem $\Theta_T(q) = F_T(q,p) = \min\{m(q), \Theta(p)\}$.

Este clar că $(T(H), \Theta_T)$ este o mulţime indexată.

Teorema III.5.6. Fie (H,Θ) o mulţime indexată, (H, α_Θ) mulţimea calibrată corespunzătoare şi $(T(H), \alpha_T)$ mulţimea calibrată indusă de (H, α_Θ). Atunci pentru $\forall q \in T(H)$, $\alpha_T(q) = \alpha_{\Theta_T}(q)$.

Deci $(T(H), \alpha_T) = (T(H), \alpha_{\Theta_T})$.

Demonstraţie. Avem pentru $\forall q \in T(H)$, $\alpha_T(q) \subseteq \alpha_{\Theta_T}(q)$.

Într-adevăr, fie $q' \in \alpha_T(q)$, atunci $q' \in [q] \cap T(\alpha(p))$ pentru $p \in H$ cu $q \in T(\{p\})$. Deci $p = uq$ şi $u'q' \in \alpha_\Theta(p)$. Dar atunci $uq \in \alpha_\Theta(p)$, $u'q' \in \alpha_\Theta(p)$ şi deci $0 \leq \rho(uq, u'q') = \rho(u,u') + \rho(q,q') \leq \Theta(p)$. In particular $\rho(q,q') \leq \Theta(p)$. Avem şi $\rho(q,q') \leq m(q)$ şi deci $\rho(q,q') \leq F_T(q,p) \leq \Theta_T(q)$ şi $q' \in \alpha_{\Theta_T}(q)$.

Invers, vom arăta că $\alpha_{\Theta_T}(q) \subseteq \alpha_T(q)$, pentru orice $q \in T(H)$. Pentru $q \in T(H)$ alegem $q' \in \alpha_{\Theta_T}(q)$.

Atunci $\rho(q,q') \leq \Theta_T(q)$. Există $p \in H$ astfel încât $\rho(q,q') \leq \Theta_T(q) = F_T(q,p) = \min\{m(q), \Theta(p)\} \leq \Theta(p)$ şi $p = uq$. Dar atunci $\rho(uq, uq') \leq \Theta(p)$ şi deci $uq' \in \alpha_\Theta(p)$ de unde $q' \in \alpha_T(q)$. ∎

Exemplul III.5.1. Fie $I = \{0,1\}$ şi $H = \{001, 1010, 01010\}$. Codul simplu (H, ι) nu-i sincronizabil. Avem $T(H) = H \cup \operatorname{Suf}_p H = \{001, 01, 1, 1010, 010, 10, 0, 01010\}$,

Iar

$R_0(H,\iota;T(H),\iota)$	$R_1(H,\iota;T(H),\iota)$	$R_2(H,\iota;T(H),\iota)$	$R_3(H,\iota;T(H),\iota)$	$R_4(H,\iota;T(H),\iota)$
0	01	010	10	10
1	1010	10		
01	010			
10	10			
001				
010				
1010				
01010				

Prin urmare $R_3(H,\iota;T(H),\iota) = R_{n+3}(H,\iota;T(H),\iota) = \{10\} \neq \emptyset$ și codul (H,α) nu-i sincronizabil.

Exemplul III.5.2 [Hartnett [30]]. Fie $I = \{0,1\}$ și $H = \{010, 110111\}$, cu indexarea $\theta : H \to N$ dată de $\theta(010) = 1$ și $\theta(110111) = 0$. Apoi $g(0,0) = g(1,1) = 0$ iar $g(1,0) = 1$.

Aplicația $\rho : H \times H \to N$ extinsă din aplicația g este dată în tabloul:

ρ	010	110111
010	0	1
110111	1	0

Determinînd aplicația de calibrare corespunzătoare α_θ, obținem:

$$\alpha_\theta(010) = \{010, 110, 000, 011\}$$

iar

$$\alpha_\theta(110111) = \{110111\}.$$

Avem $H_1 = \{111\}$, iar $H_2 = \emptyset$.

Dăm numai o prezentare a rezultatelor testului de sincronizare. Avem:

1. (H,θ) dă $(T(H),\theta_T)$ prin teorema III.5.6
2. (H,θ) și $(T(H),\theta_T)$ dau prin construcția (H_1,θ_1)
3. (H,θ) și (H_1,θ_1) dau prin construcție (H_2,θ_2)

- -

n + 2.(H,Θ) şi (H_n,Θ_n) dau prin construcţie (H_{n+1},Θ_{n+1})

Dacă mulţimile calibrate (H_n,Θ_n) şi (H_{n+1},Θ_{n+1}) coincid atunci $(H_n,\Theta_n) = (H_{n+k},\Theta_{n+k})$ pentru $\forall k \in N$.

Rezultatele obţinute prin calcul le dăm în tabloul următor:

H	Θ	T(H)	Θ_T	H_1	Θ_1	H_2	Θ_2	H_3	Θ_3	- - - - -
010	1	010	1							
110111	0	110111	0							
		0	1	0	0	0	0	0	0	
		1	0	1	0	1	0	1	0	
		10	1	10	1	10	1	10	1	
		11	0	-	-	-	-	-	-	
		111	0	111	0	-	-	-	-	- - - - -
		0111	0	0111	0	0111	0	0111	0	
		10111	0	10111	0	10111	0	10111	0	

Se observă că $(H_2,\Theta_2) = (H_3,\Theta_3) = (H_n,\Theta_n)$ pentru orice $n \geq 2$. Cum $H_2 \neq \emptyset$ urmează că codul (H, α) nu este sincronizabil.

x

x x

În tabloul următor scoatem în evidenţă caracterizări explicite ale codurilor de tipurile introduse, comparînd între ele afirmaţii "asemănătoare".

Proprietatea codului H	Afirmaţie echivalentă
Cod corector	$\alpha(H) \cap \alpha_n(R_n(H,\alpha;H,\alpha)) = \emptyset, \forall n \in N^*$
Cod decodabil	$\alpha(H) \cap \alpha_n(R_n(H,\alpha;H,\alpha)) = \emptyset, \forall n \in N^*$ $\exists n_0 \in N^*$, $R_{n_0}(H,\alpha;H,\alpha) = \emptyset$
Cod sincronizabil	$\alpha(H) \cap \alpha_n(R_n(H,\alpha;H,\alpha)) = \emptyset, \forall n \in N^*$ $\exists n_0 \in N^*$, $R_{n_0}(H,\alpha;\mathrm{Sup}\,\alpha(H),\iota) = \emptyset$

Anexa A. Semigrupuri libere

Fie I o mulțime cel mult numărabilă numită alfabet. Orice element $i \in I$ se numește literă sau simbol.

Definiția A.1 Un cuvînt peste alfabetul I este un șir finit de simboluri din I, $p = \{i_1, \ldots, i_n\}$, $i_j \in I$, $j = \overline{1,n}$.

Convenim să notăm $p = i_1 \ldots i_n$.

Lungimea cuvîntului p este $\ell(p) = \ell(i_1 \ldots i_n) = n$, adică numărul simbolurilor din I care apar în cuvîntul p.

In mulțimea cuvintelor peste alfabetul I se introduce operația de concatenare (juxtapunere). Astfel are loc:

Definiția A.2 Cuvîntul obținut prin concatenare (juxtapunere) din cuvintele $p = i_1 \ldots i_n$, și $q = i'_1 \ldots i'_m$ este cuvîntul

$$pq = i_1 \ldots i_n \, i'_1 \ldots i'_m.$$

Avem $\ell(pq) = \ell(p) + \ell(q)$.

Observația A.1. Mulțimea tuturor cuvintelor peste un alfabet I, dotată cu operația de concatenare este un semigrup numit semigrup liber generat de I și notat cu I^*. Alfabetul I se mai numește mulțimea de generatori ai semigrupului liber I^*.

In semigrupul liber I^* există element neutru la operația de concatenare, cuvîntul vid (nul) e cu $\ell(e) = 0$.

Avem $ep = pe = p$, $\forall p \in I^*$.

Dacă $p \in I^*$, convenim să notăm cu $p^n = \underbrace{p \ldots p}_{n}$ și $p^0 = e$.

Intr-un semigrup liber este valabilă proprietatea de simplificare, astfel dacă $pq_1r = pq_2r$, atunci $pq_1 = pq_2$, $q_1r = q_2r$ și $q_1 = q_2$.

Denumirea de semigrup liber este justificată prin:

Teorema A.1. Orice aplicație $\varphi : I \to S$, unde S este un semigrup oarecare se extinde în mod unic la un homomorfism

$\varphi : I^{\#} \longrightarrow S$.

Demonstrație. Fie $p \in I^{\#}$. Vom defini $\varphi_1(p) = \varphi_1(i_1 \ldots i_n) \overset{def}{=} \varphi(i_1) \ldots \varphi(i_n)$. Se constată imediat că aplicația φ_1 astfel obținută este un homomorfism de semigrupuri, care coincide pe generatorii semigrului liber $I^{\#}$, cu aplicația φ.

Să presupunem că ar exista un homomorfism $\varphi_2 : I^{\#} \to S$, astfel încît restricția lui φ_2 la I să coincidă cu restricția lui φ_1 la I, deci cu φ.

Mulțimea E definită prin $E = \{p \mid \varphi_1(p) = \varphi_2(p)\}$ este un subsemigrup al lui $I^{\#}$.

Să observăm mai întîi că $E \neq \emptyset$ deoarece $I \subseteq E$.

Apoi fie $p, q \in E$. Atunci $\varphi_1(pq) = \varphi_1(p)\ \varphi_1(q) = \varphi_2(p) \cdot \varphi_2(q) = \varphi_2(pq)$, deci $pq \in E$.

Cum E este un subsemigrup al lui $I^{\#}$, $E \subseteq I^{\#}$, care conține mulțimea de generatori ai semigrupului liber $I^{\#}$, urmează $E = I^{\#}$. ■

Observația A.2. Unei mulțimi $A \subset I^{\#}$, i se poate ataşa subsemigrupul lui $I^{\#}$, generat de A, adică cel mai mic subsemigrup al lui $I^{\#}$, care conține mulțimea A și pe care îl vom nota cu S(A).

Deoarece mulțimea subsemigrupurilor lui $I^{\#}$, care-l conțin pe A, nu-i vidă, existînd cel puțin $I^{\#}$, și intersecția de subsemigrupuri ale lui $I^{\#}$, este tot un subsemigrup al lui $I^{\#}$ avem

$$S(A) = \bigcap T .$$

T subsemigrup în $I^{\#}$ și $A \subseteq T$.

Un element din S(A) este un cuvînt din $I^{\#}$, obținut prin concatenarea unor cuvinte din A.

Pe de altă parte, lui A i se poate ataşa semigrupul liber generat de A, pe care îl vom nota cu $A^{\#}$. Un element

din A^* este un şir finit de cuvinte din A, $m=(p_1,\dots,p_k)$, $p_j \in A$, $j = \overline{1,k}$ şi se numeşte propoziţie pe A, iar m $m_1 = (p_1,\dots,p_k,p'_1,\dots,p'_s)$ dacă $m,m_1 \in A^*$ şi $m = (p_1,\dots,p_k)$, iar $m_1 = (p'_1,\dots,p'_s)$.

Lungimea unei propoziţii $m \in A^*$, $m=(p_1,\dots,p_k)$ este $\ell(m) = k$, adică numărul cuvintelor din şir.

Dacă $m \in A^*$, atunci convenim să notăm prin m(1), m(2), ...m(*), primul cuvînt din m, al doilea cuvînt din m şi respectiv ultimul cuvînt din m, şi vom mai scrie m=m(1)m(2)...m(*).

Legătura dintre cele două semigrupuri care se pot ataşa unei mulţimi $A \subset I^*$ este dată de:

Teorema A.2. Aplicaţia $\wedge : A^* \to S(A)$ definită prin $\hat{m} = p_1 \dots p_k$ dacă $m = (p_1,\dots,p_k)$ este homomorfism surjectiv de semigrupuri. Avem $\hat{A}^* = S(A)$.

Demonstraţie. Este suficient să observăm că $\widehat{m_1 m_2} = \hat{m}_1 \hat{m}_2$, $\forall m_1, m_2 \in A^*$ şi că pentru orice element $v \in S(A)$ există $m \in A^*$ cu $v = \hat{m}$.

Observaţia A.3. Homomorfismul " $\wedge$ " este determinat prin corespondenţa $(p) \longrightarrow p$, $\forall p \in A$. Vom identifica $(p) \in A^*$ cu $p \in A \subset S(A)$.

Dacă $m \in A^*$, atunci $\ell(\hat{m})$ se mai numeşte întinderea propoziţiei m, şi este deci numărul tuturor literelor din toate cuvintele din şirul m.

Astfel, dacă $m=(p_1,\dots,p_k)$, atunci $\ell(m) = k$, iar întinderea $\ell(\hat{m}) = \ell(p_1) + \dots + \ell(p_k)$.

Ne vom ocupa în continuare de unele proprietăţi ale cuvintelor unui semigrup liber .

Teorema A.3. Dacă $p,q,r \in I^*$ şi există $n_1 \in N^*$ cu

$$pq^{n_1} = r^{n_1}p,$$

atunci

$$pq^{n} = r^{n}p \ , \ \forall\, n \in N^{*}.$$

Demonstrație. Să observăm mai întîi că dacă $q = e$, atunci și $r = e$ (folosind proprietatea de simplificare) și teorema se verifică banal. La fel dacă $r = e$. Fie deci $q, r \neq e$. Vom arăta prin inducție după h, că

$$pq^{hn_1} = r^{hn_1}p.$$

Pentru $h = 1$, obținem ipoteza teoremei. Să presupunem că $pq^{hn_1} = r^{hn_1}p$. Atunci $pq^{(h+1)n_1} = pq^{hn_1+n_1} = pq^{hn_1}q^{n_1} =$

$= r^{hn_1}pq^{n_1} = r^{hn_1}r^{n_1}p = r^{(h+1)n_1}p.$

Există $n_2 \in N^{*}$, $n_2 = k_1 n_1$ și astfel încît $\ell(p) \leq \ell(r^{n_2})$. (aici intervine faptul că $\ell(r) \geqslant 1$). Avem $pq^{n_2} = r^{n_2}p$, de unde rezultă $p = r^{t}r'$ cu $r = r'r''$ și $0 \leq t \leq n_2$.
Atunci $r^{t}r'q^{n_2} = r^{n_2}r^{t}r'$, sau simplificînd cu r^{t}, $r'q^{n_2} = r^{n_2}r'$ sau încă

$$r'q^{n_2} = (\underbrace{r'r''\ r'r''\ldots r'r''}_{n_2})r',$$

de unde prin simplificare cu r',

$$q^{n_2} = r''r'\ r''r'\ldots r''r' = (r''r')^{n_2},$$

deci $q = r''r'$. Astfel pentru orice $n \in N^{*}$, avem

$$pq^{n} = r^{t}r'\,(r''r')^{n} = r^{t}(r'r'')^{n}\,r' = r^{t}r^{n}r' = r^{n}r^{t}r' =$$

$$= r^{n}p. \quad \blacksquare$$

Teorema 4.4. Dacă $p, q \in I^{*}$ și $pq = qp$, atunci există $r \in I^{*}$ și $n_1, n_2 \in N$ astfel încît $p = r^{n_1}$ și $q = r^{n_2}$, cu alte cuvinte dacă două elemente din un semigrup liber sînt comutabile, ele sînt puteri ale unui aceluiași element din semigrup.

Demonstrație. Vom proceda prin inducție după $\ell(pq)$. Dacă $\ell(pq) = 0$, atunci $p = q = e$ și teorema este adevărată luînd $r = e$. Dacă $\ell(pq) = 1$, atunci $p = e$ sau $q = e$ și teorema se verifică luînd $r = q$, $n_1 = 0$, $n_2 = 1$ și respectiv $r = p$, $n_1 = 1$ și $n_2 = 0$. Să presupunem teorema adevărată pentru $\ell(pq) < n$, și fie $pq = qp$ cu $\ell(pq) = n$. Dacă $\ell(p) = 0$, atunci $p = e$ și luăm $r = q$, $n_1 = 0$, $n_2 = 1$. Putem presupune deci $0 < \ell(p) < \ell(q)$. Atunci $q = pq'$ și $ppq' = pq'p$, de unde prin simplificare cu p, obținem $pq' = q'p$ și $\ell(pq') < \ell(pq) = n$. Conform cu ipoteza inductivă există $r \in I^*$ și $p = r^{n_1}$, $q' = r^n$. Prin urmare $q = pq' = r^{n_1+n} = r^{n_2}$. ■

Teorema A.5. Dacă $p_1p_2p_3 \in I^*$ și $p_1p_2p_3 = p_3p_2p_1$ cu $0 < \ell(p_1) < \ell(p_3)$, atunci există $r \in I^*$ și întregul $n \geq 2$, astfel încît $p_3p_2 = r^n$.

Demonstrație. Este clar că $p_3 = p'_3 \neq e$, de unde $p_1p_2p_3 = p_1p_2p'_3p_1 = p'_3p_1p_2p_1$, de unde, prin simplificare prin p_1, obținem $(p_1p_2)p'_3 = p'_3(p_1p_2)$, deci elementele p_1p_2 și p'_3 sînt comutabile. În baza teoremei A.4, există $r \in I^*$ cu $p_1p_2 = r^{n_1}$ și $p'_3 = r^{n_2}$. Deoarece $\ell(p_1) > 0$ și $\ell(p'_3) > 0$, avem $n_1 \geq 1$, $n_2 \geq 1$. Atunci $p_3p_2 = p'_3p_1p_2 = r^{n_1+n_2} = r^n$, $n \geq 2$. ■

Teorema A.6. Dacă $p_1, p_2p_3 \in I^*$ și $p_1p_2 = p_3p_1 \neq e$, atunci există $h \in N^*$ și $u, v \in I^*$ astfel încît $p_1 = (vu)^hv$, $p_2 = uv$, $p_3 = vu$.

Demonstrație. Să presupunem mai întîi că $\ell(p_1) \leq \ell(p_2)$. Atunci $p_2 = up_1$, de unde $p_3 = p_1u$ și teorema se verifică luînd $p_1 = v$ și $h = 0$.

Dacă $\ell(p_1) \geq \ell(p_2)$ vom proceda prin inducție asupra lui $\ell(p_1)$. Cazul inițial, $\ell(p_1) = \ell(p_2)$, este verificat în baza celor de mai sus.

Să presupunem afirmația adevărată pentru $\ell(p_1) < n$ și fie $\ell(p_1) = n > \ell(p_2)$. Atunci $p_1 = p'_1p_2$ cu $0 < \ell(p'_1) < \ell(p_1)$.

Avem $p'_1p_2p_2 = p_3p'_1p_2$, de unde $p'_1p_2 = p_3p'_1$ şi în baza ipotezei inductive există $u,v \in I^*$ astfel încît $p'_1 = (vu)^k v$, $p_2 = uv$, $p_3 = vu$. Atunci $p_1 = p'_1p_2 = (vu)^k v\, u\, v = (vu)^{k+1}v$. ■

Vom introduce acum noţiunile de prefix, sufix şi infix ale unui cuvînt dintr-un semigrup liber.

Definiţia 4.3. Fie $w \in I^*$ cu $w = prs$. Atunci p se numeşte un prefix al lui w, r un infix al lui w, iar s un sufix al lui w. Dacă $p \neq e$, w şi p este atunci un prefix propriu, dacă $s \neq e, w$, s este un sufix propriu ; dacă r nu-i prefix sau sufix al lui w, atunci r este un infix propriu.

Este convenabil să introducem aplicaţiile $Pref : \mathcal{P}^c(I^*) \to \mathcal{P}(I^*)$ şi $Suf : \mathcal{P}^c(I^*) \to \mathcal{P}(I^*)$ date respectiv prin:

$$Pref\, A = \{p \mid p \in I^*,\ \exists\, q \in I^*,\ pq \in A\},$$

şi

$$Suf\, A = \{q \mid q \in I^*,\ \exists\, p \in I^*,\ pq \in A\},$$

unde am notat prin $\mathcal{P}^c(I^*) = \{A \mid A \subseteq I^* \setminus \{e\}\}$.

Mulţimile $Pref\, A$ şi $Suf\, A$ sînt respectiv mulţimea prefixelor şi mulţimea sufixelor pentru cuvintele din A.

Vom nota prin $Prefp\, A$ (= $Pref\, A \setminus (A \cup \{e\})$, iar $Sufp\, A$) este $Sufp\, A = Suf\, A \setminus (A \cup \{e\})$. Prin urmare $Prefp\, A$ este mulţimea prefixelor proprii ale cuvintelor din A, care nu sînt cuvinte din A, iar $Sufp\, A$ este mulţimea sufixelor proprii ale cuvintelor din A, care nu sînt cuvinte $\in A$.

Mulţimea $Inf\, A = \{r \mid r \in I^*,\ \exists p \in I^*,\ \exists s \in I^*,\ prs \in A\}$ este mulţimea infixelor cuvintelor din A, iar $Infp\, A = Inf\, A \setminus (A \cup \{e\})$.

Mulţimea $Q(A) = Pref\, A \cap Suf\, A$ este mulţimea sfixelor cuvintelor din A. Să observăm că $Q(A) \neq \emptyset$, deoarece cel puţin $e \in Q(A)$.

Observatia A.1. Deoarece A este un semigrup liber se poate vorbi de prefixele, sufixele şi infixele elementelor din A , deci a propoziţiilor pe A.

Astfel, pentru $m_1, m_2 \in A$, avem $m_1 \in Pref\{m_2\}$, dacă există $m \in A$ cu $m_2 = m_1 m$. Apoi $m_1 \in Suf\{m_2\}$ dacă există $m \in A$ cu $m_2 = m\, m_1$. In sfîrşit $m_1 \in Inf\{m_2\}$, dacă există $m, m' \in A$ cu $m_2 = m\, m_1 m'$. Analog se poate vorbi de prefixe, sufixe şi infixe proprii pentru propoziţiile pe A.

Teorema A.2. Fie $A \subset I^* \setminus \{e\}$ şi $m_j \in A^*$, $j = \overline{1,4}$. Dacă $m_1 m_2 = m_3 m_4$ şi $\ell(\hat{m}_1) \leq \ell(\hat{m}_3)$, atunci $m_1 \in Pref\{m_3\}$.

Demonstratie. Fie $m_1 m_2 = m_3 m_4$ şi $l(\hat{m}_1) < l(\hat{m}_3)$. Pentru ca $m_1 \in Pref\{m_3\}$, trebuie să avem $\ell(m_1) \leq \ell(m_3)$. Să presupunem contrariul, deci că $\ell(m_1) > \ell(m_3)$. Atunci, deoarece în semigrupul liber A^* este valabilă regula de simplificare, m_3 este un prefix al lui m_1, deci orice cuvînt din propoziţia m_3 este şi un cuvînt din propoziţia m_1, adică $m_3(1) = m_1(1), \ldots, m_3(\star) = m_1(k)$, şi prin urmare $\ell(\hat{m}_3) < \ell(\hat{m}_1)$, ceea ce contrazice ipoteza teoremei. Rămîne deci $\ell(m_1) \leq \ell(m_3)$ şi astfel $m_1 \in Pref\{m_3\}$. ∎

Fie $A, B \subset I^* \setminus \{e\}$ şi $m \in A^*$; $n \in B^*$.

Definitia A.4. Propoziţia $m \in A^*$ preegalează propoziţia $n \in B^*$, dacă pentru orice $m_1, m_2 \in A^*$, cu $m = m_1 m_2$, există $n_1, n_2 \in B^*$ cu $n = n_1 n_2$ şi $\ell(\hat{m}_1) = \ell(\hat{n}_1), \ell(\hat{m}_2) = \ell(\hat{n}_2)$. Vom nota $m \rightleftharpoons n$.

Cu alte cuvinte avem $m \rightleftharpoons n$, dacă la orice descompunere a lui m în propoziţii corespunde o descompunere al lui n în propoziţii care au corespunzător aceeaşi întindere ca şi propoziţiile lui m.

Observatia A.5. Preegalarea între propoziţii este o relaţie reflexivă şi tranzitivă (de preordine). Ea permite compararea lungimii cuvintelor ce formează propoziţiile, deci compararea "poziţiilor virgulelor" între cuvintele din propoziţii.

Dacă se cunoaşte împărţirea în cuvinte a propoziţiei m, atunci se pot descompune în propoziţii de întindere egală cu lungimea cuvintelor lui m, propoziţiile n, pe care m le preegalează.

Teorema A.8. Fie $m = (p_1,\dots,p_r) \in A^*$ şi $n \in B^*$. Avem $m \dashv n$ dacă şi numai dacă există $n_1,\dots n_r \in B^*$ astfel încît $n = n_1 \dots n_r$ şi $\ell(p_j) = \ell(\hat{n}_j)$, $j = \overline{1,r}$.

Demonstraţie. Se procedează prin inducţie după $r = \ell(m)$. Dacă $r = 1$, atunci $m = (p_1) = p_1 \in A$ şi $m \dashv n$, dacă şi numai dacă $\ell(p_1) = \ell(\hat{n})$.

Să presupunem teorema adevărată pentru $r = h$ şi să trecem la $h + 1$. Fie deci $m = (p_1,\dots,p_h,p_{h+1}) \in A^*$ şi să considerăm descompunerea $m = (p_1\dots,p_h)(p_{h+1})$; atunci $m \dashv n$, dacă şi numai dacă există $n', n_{h+1} \in B^*$ cu $n = n' n_{h+1}$ şi $\ell(\overline{(p_1,\dots,p_h)}) = \ell(\hat{n}')$, iar $\ell(p_{h+1}) = \ell(\hat{n}_{h+1})$.

Dar atunci $(p_1,\dots,p_h) \dashv n'$ şi conform ipotezei inductive $n' = n_1 \dots n_h$ cu $\ell(p_j) = \ell(\hat{n}_j)$, $j = \overline{1,h}$, şi deci $n = n_1 \dots n_h\, n_{h+1}$ cu $\ell(p_j) = \ell(\hat{n}_j)$, $j = \overline{1,h+1}$. ∎

Consecinţa A.1. Dacă $m \dashv n$, atunci $\ell(m) \leq \ell(n)$, deoarece propoziţiile n_j, $j = \overline{1,r}$, pot fi formate din mai multe cuvinte, deci $\ell(n_j) \geq 1$.

Consecinţa A.2. Dacă propoziţia $m_1 m_2 \in A^*$ cu $m_1, m_2 \in A^*$ preegalează propoziţia $n \in B^*$, atunci există $n_1, n_2 \in B^*$ cu $n = n_1 n_2$ şi $m_j \dashv n_j$, $j = \overline{1,2}$.

Definiţia A.5. Propoziţia $m \in A^*$ egalează propoziţia $n \in B^*$ dacă $m \dashv n$ şi $n \dashv m$. Vom nota $m \vdash\!\dashv n$.

Observaţia A.6. Egalarea între propoziţii este o relaţie de echivalenţă (reflexivă, simetrică şi tranzitivă).

Observaţia A.7. Dacă $m \models n$, atunci $\ell(m) = \ell(n)$, deci propoziţiile m şi n sînt formate din acelaşi număr de cuvinte. Mai mult, dacă se cunoaşte împărţirea în cuvinte a propoziţiei m (deci poziţiile "virgulelor" dintre cuvintele lui m), atunci se poate descompune în cuvinte (deci distribui virgulele), orice propoziţie n cu $m \models n$. In adevăr, dacă $m = (p_1, \ldots, p_r)$ atunci $n = n_1 \ldots n_r$ şi cum $\ell(m) = \ell(n)$, avem $\ell(n_j) = 1$, $j = \overline{1,r}$, deci n_j sînt cuvinte.

Din $\ell(p_j) = \ell(n_j)$, $j=\overline{1,r}$, urmează $\ell(m(1)) = \ell(n(1))$, $\ldots, \ell(m(*)) = \ell(n(*))$, deci cuvintele cu acelaşi indici din propoziţiile m şi n au lungimile egale.

Dacă pentru două propoziţii $m \in A^*$ şi $n \in B^*$, avem $\ell(m) = \ell(n)$ şi $\ell(m(1)) = \ell(n(1)), \ldots, \ell(m(*)) = (n(*))$, atunci evident $m \models n$.

Ca atare avem $m \models n$, dacă şi numai dacă propoziţiile m şi n sînt formate din acelaşi număr de cuvinte şi cuvintele cu acelaşi indice au lungimile egale.

Bibliografie

1. Abramson, N. - Information Theory and coding.Mc. Graw-Hill, New-York, 1963.

2. Arquette, L.K.; Hartnett, W.E. A study of error -correcting codes. II.decodability properties.P.M.L.Scientific Report,No.9, 3826, 1966.

3. Arquette, L.K.; Calabi, L., Hartnett, W.E. A study of error - correcting codes.III, synchronizability and comma freedom.PML Scientific Report No.1,0030, 1966.

4. Bandyopadhyay, G. -A simmple proof of the decipherability criterion of Sardinas and Patterson.Information and Control 6 (1963), 331-336.

5. Banerji, R. - On constructing group codes. Information and Control, 4 (1961), 1-14.

6. Blum, E.D.- Some fundamental properties of error.-correcting codes. Technical Memorandum No.15, 3826 (1965 b) Parke Math.Lab., Inc.,Carlisle, Mass.

7. Calabi, L. - Combinatorial properties of variable - length error-correcting codes with an Appendix by J.A.Riley. PML.Inc.,Scientific Report Np 2,3826, 1964.

8. " On the computation of Levenshtein's distances.TM-9-0030,1967,Parke Math.Lab. Inc.,Carlisle,Mass.

9. Calabi, L., Arquette, L.K. - Basic properties of codes PML,Inc., Technical Memorandum No.14, 3826, 1965.

21. E v e n, S. - Tests for unique decipherability IEEE Trans.Inform.Theory IT-9 (1963),1o9-112.

22. " Test for synchronizability of finite automata and variable length codes. IEEE Trans.Inform.Theory IT - 1o (1964), 185-189.

23. G i l b e r t, E.N.- Synchronization of binary messages. IRE Trans. IT - 6, (196o),47o-477.

24. G i l b e r t,E.N.; M o o r e, E.F.- Variable length binary encoding.Bell System Tech J. 38 (1959), 933-968.

25. G l e b s k i j, J u. V. -Kodirovanie s pomoščʹju konečnyh avtomatov. D.A.N. 141, 5 (1961),1o54-1o57.

26. G o l o m b, S.W.; G o r d o n, B.- Codes with bounded synchronization delay. Information and Control 8 (1965),355-372.

27. G o l o m b, S.; G o r d o n,B.; W e l c h .L.- Comma - free codes.Canad.J.Math.1o (1958), 2o2-2o9.

28. H a r n e t t, W.E.-Generalization of tests for certain properties of codes. PML Scientific Report No.7, 3826, 1966.

29. " Generalization of codes and strong code properties. PML Technical Memorandum No.1, 0030, 1967.

3o. " Generalizations of tests for certain properties of variable length codes.Information and control 13 (1968), 2o-45.

31. H a t c h e r, T.R.-On a family of error - correcting and synchronizable codes.PML Scientific Report No.4, 0030, 1968.

32. Hu f f m a n, D.A.- A method for construction of minimum redundancy codes.Proc.I.R.E.4o (1952),1o98-1101.

43. L e v e n ş t a j n , V.I.- Ob izbytočnosti i zamedlenii razdelitogo kodirovanija natural'nyh cisel. Sb.Problemy kibernetiki 20 (1968), 173-179.

44. L j a p i n, E.S.- Polugruppy.Gosud.Izd.Fiz.-Mat,.Lit. Moskva,1960.

45. L y n d o n, R.C.; S c h ü t z e n b e r g e r, M. P.- The equation $a^M=b^Nc^P$ in a free group. Michigan Math.J. 9 (1962), 289-298.

46. M a r k o v, A.A.- Ob alfavitnom kodirovanii.I.D.A.N. 132, 3 (1961), 521 - 523
II D.A.N. 139, 3 (1961) 560-561.

47. " Nerekurrentnoe kodirovanie.Sb. "Problemy kibernetiki" vyp.8.M.,Fizmatgiz., 1962.

48. " Kody c korrekciej ošibok Izv.vuzov Radiofizika 2, 1963.

[illegible]. " Uslovija polnoty dlja neravnomernyh kodov.I. Sb."Problemy Kidernetiki,9 (1963), 327-331.

50. " Neravnomernye kody s ispravleniem ošibok. Sb."Problemy Kibernetiki, vyp.8, M.(1964),137-153.

51. " Uslovija polnoty dlja neravnomernyn kodov.II.Sb. "Problemy kibernetiki, 19 (1967),307-309.

[illegible]. " O nekotoryh svojstva beskonečnyh prefiksnyh kodov.Problemy peredači informacii IV (1970), 97-98.

53. M a r k u s, R.S., S c h ü t z e n b e r g e r, M.P. - Full decodable code word sets. IRE Trans. Inform.Theory II. 5 (1959), 12-15.

54. Mc M i l l a n, B.- Twoinequalities implied by unique decipherability.IRE Trans. I T - 2 (1956),115-116.

55. M y r v a a g n e s, E.- Eighteen hundred selected two-word codes.PML, Inc., Scientific Report No.3, 3826,1965.

56. " Some binary codes for error-correction and synchronization. PML, Inc.Scientific Report Nr.4, 3826, 1965.

57. N e u m a n n, P.- On a class of efficient error-limiting variable-length codes. IRE Trans. IT 8 (1962),260-266.

58. " Efficient error - limiting variable - length codes. IRE Trans. IT-8 (1962), 292-304.

59. N i v a t, M.- Eléments de la théorie générale des codes. In "Automata Theory" (E.R.Caianiello, ed).Academic Press. New-York, London,1966, 278-294.

60. P a t t e r s o n, G.N.- Linear syntactical bases. J.Symbolic Logic 16 (1951),236.

61. R a b i n, M.O.& S c o t t, D.- Finite automata and their decision problems .IBM J.Res.Develop.3 (1959),114-125.

62. R e i s c h e r, C.; S i n o v i c i,D.- Lattice characterizations for codes. Acad.Naz. dei Lincei,Rendiconte della classe di Scienze fisiche,matematiche e naturale ,serie VII,vol.LII,(1972), 287-290.

63. " Une condition nécessaire et suffisante d'unique déchiffrabilité. An.St.Univ.Iaşi.T.XIX(1974)(sub tipar)

64. R i l e y, J. A.- The Sardinas-Patterson and Levenshtein theorems. Information and Control 10 (1967), 120-136.

65. S a r d i n a s, A.A.; P a t t e r s o n, G.W.- A necessary and sufficient condition for the unique decomposition of codes messages. Research Division Report, 50-27, 1950, Moore School of Electrical Engineering, University of Pennsylvania.

66. " A necessary and sufficient condition for the unique decomposition of code messages. IRE Intern. Conv. Record 8 (1953), 104-108.

67. S c h o l t z, R.A.- Codes with synchronization ability. IEEE Trans. I T - 12 (1966), 135-142.

68. S c h ü t z e n b e r g e r, M.P.- On an application of semigroup methods to some problems in coding. IRE Trans. Inform. Theory I T-2 (1956), 47-60.

69. S e l l e r s, F.F.- Bit loss and gain correction code. IRE Trans. I T-8, 1 (1962), 35-38.

70. S h a n n o n, C.E.- A mathematical theory of communication. Bell System Tech. J. 27 (1948), 379-423, 623-656.

71. S h e p h e r d s o n, J.C.- The reduction of two-way automata to one-way automata. IBM J. Res. Develop. 3 (1959), 198-200.

72. S l e p i a n, D.- A class of binary signaling alphabets. Bell Telephone System Technical Journal Vol. 35 (1956), 203-234.

73. S m o r o d i n s k y, M.- On infinite decodable codes. Information and Control, 11 (1968), 5-6, 607- 612.

74. S p ă t a r u, A l. - Teoria transmisiunii informaţiei. Coduri şi decizii statistice. Editura Tehnică, Bucureşti, 1971.

75. W o l f o w i t z, J. - Coding theorems of Information theory Prentice - Hall, Englewood Cliffs, N.J. 1961.

Scanned with OKEN Scanner

INDICE ALFABETIC

Alfabet 116
algoritmul lui Sardinas-Patterson 54
aplicaţie de admisibilitate 12
" calibrare 80
" indusă 112
" decodificare 17
" scindare 17
Canal 7
" cu zgomot 8
" fără zgomot 8
cîtul de complexe 44
" de cuvinte 44
cod pe alfabetul I 12
" binar 12
bloc 8
" corector 26
" cu întîrziere mărginită 28
" cu lungime variabilă 8
" cu unică descifrabilitate 26
" decodabil 28
" extins 14
" finit 12
indexat 84
" infinit 12
" simplu 12
" sincronizabil 30
complexul rezidual al unui complex 45

complexul rezidual al unui complex în raport cu alt complex 45
concatenare 116
cuvînt 116
" cod 13
" nul 116
" vid 116
cuvinte compatibile 93
Dispozitiv de codificare 7
" " 8
domeniu de admisibilitate 13
Egalare 123
egalitate ireductibilă 48
erori elementare 9
" de sincronizare 8
" substituţie 8
" ştergere 9
" transmitere 8
Homomorfism de cifrare 39
" corectare 16
" decodificare 17
" scindare 17
Indexare 84
infix 121
" propriu 121
Întinderea unei propoziţii 118
întîrzierea codului 28
" de sincronizare a codului 31
Juxtapunere 116
Quasi-metrică 85

Literă 116
lungimea unui cuvînt 116
" unei propoziţii 118
Mesaj 7
model de eroare 13
mulţimea afixelor 121
" calibrată 80
" " extinsă 82
" " incusă 112
" " simplă 82
" de generatori 116
" de şiruri admisibile 14
" indexată 84
" infixelor 121
" " proprii 121
" prefixelor 121
" " proprii 121
" sufixelor 121
" " proprii 121
Preegalare 122
prefix 121
" propriu 121
propoziţie 118
" admisibilă 13
proprietate extensibilă 16
" de simplificare 116
" de unică descifrabilitate 26
" " " ciclică 60
" " " infinită 59

Relaţia de extindere 15
residiul la dreapta 40
" la stînga 40
Semigrup liber 116
simbol 116
subsemigrup generat de o mulţime de cuvinte 117
sufix 121
" propriu 121
sursa de informaţie 7

Scanned with OKEN Scanner